Michigan Law Review

Volume 102 | Issue 5

2004

The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution

Orin S. Kerr
George Washington University Law School

THE FOURTH AMENDMENT AND NEW TECHNOLOGIES: CONSTITUTIONAL MYTHS AND THE CASE FOR CAUTION

*Orin S. Kerr**

TABLE OF CONTENTS

* Associate Professor, George Washington University Law School. B.S.E. 1993, Princeton; M.S. 1994, Stanford; J.D. 1997, Harvard. Thanks to Ronald Allen, Patricia Bellia, Paul Schiff Berman, Paul Butler, Dan Markel, Richard Pierce, Neil Richards, Jeffrey Rosen, Steve Saltzburg, Michael Selmi, David Sklansky, Chris Slobogin, Daniel Solove, Carol Steiker, Peter Swire, and the participants in the George Washington University Law School workshop and the May Gathering for helpful comments on an earlier draft.

INTRODUCTION

The Supreme Court recently considered whether aiming an infrared thermal imaging device at a suspect's home can violate the Fourth Amendment. *Kyllo v. United States*[1] announced a new and comprehensive rule: the government's warrantless use of sense-enhancing technology that is "not in general use" violates the Fourth Amendment when it yields "details of the home that would previously have been unknowable without physical intrusion."[2] Justice Scalia's majority opinion acknowledged that the Court's rule was not needed to resolve the case before it, which dealt only with a crude infrared camera.[3] Justice Scalia justified the broad rule on the Court's need to "take the long view"[4] and protect the public from the threat of other more nefarious government surveillance technologies — including technologies yet to be invented.[5]

As surprising as *Kyllo*'s authorship may be,[6] the opinion captures the prevailing *zeitgeist* about law, technology, and privacy. When technology threatens privacy, the thinking goes, the courts and the Constitution should offer the primary response. While Congress and state legislatures may have a limited role regulating government investigations involving new technologies, the real work must be done by judicial interpretations of the Fourth Amendment.[7] The courts

1. 533 U.S. 27 (2001).

2. *Id.* at 40.

3. *See id.* at 34.

4. *Id.* at 40.

5. *See id.* at 36 ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."); *See also id.* at 36 n.3 (noting that law enforcement research teams are working on new technologies with the ultimate goal of being able to "see" through walls).

6. *See* David Cole, *Scalia's Kind of Privacy*, THE NATION, July 23, 2001, at 6-7 (expressing surprise that Justice Scalia authored the majority opinion in *Kyllo*). Recent opinions by Justice Scalia suggest that his pro-defendant stance in *Kyllo* no longer should be surprising. *See, e.g.*, Blakely v. Washington, 124 S. Ct. 2531 (2004); Hamdi v. Rumsfeld, 124 S. Ct. 2633, 2660 (2004) (Scalia, J., dissenting).

7. *See, e.g.*, Michael Adler, Note, *Cyberspace, General Searches, and Digital Contraband: the Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093 (1996) (arguing that

current Fourth Amendment doctrine gives the government too much power to use new technologies in ways that erode privacy, and that the doctrine should be reevaluated to better protect privacy); Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Trades Image and Identity*, 82 TEXAS L. REV. 1349, 1363 (2004) (contending that the scope of the Fourth Amendment protection "needs rethinking if constitutional privacy protections are to work well in twenty-first century conditions."); Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 MISS. L.J. 5, 49 (2002) (arguing that the Supreme Court should respond to the problem of new technologies by "enunciat[ing] an expansive, value-based theory of the scope of the Fourth Amendment and its role in preserving privacy and liberty"); Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 650 (1988) (arguing that recent cases "fail[] to protect privacy rights, and permits their gradual decay with each improved technological advance"); Roberto Iraola, *New Detection Technologies and the Fourth Amendment*, 47 S.D. L. REV. 8 (2002) (arguing that the Fourth Amendment should regulate the use of detection technologies); Tracey Maclin, Katz, Kyllo, *and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 51 (2002) (contending that as technology advances and allows greater means to invade privacy, the Courts should interpret the Fourth Amendment such that "the privacy and security protected by the Fourth Amendment should not depend on innovations in technology"); Raymond Shih Ray Ku, *The Founder's Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325 (2002) (arguing that the Fourth Amendment should be interpreted to require legislative authorization of government use of new technologies to better protect privacy against new technologies); Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303 (2002) (arguing that courts should focus on the result of a search on privacy interest rather than the means of its invasion in order to guarantee robust Fourth Amendment protection in new technologies); David A. Sklansky, *Back to the Future:* Kyllo, Katz, *and Common Law*, 72 MISS. L.J. 143, 210 (2002) (suggesting that "*Kyllo* is a promising decision" because it recognizes "the ways in which new technology can erode a traditional sphere of privacy" and also is sensitive to "the past, present, and the future"); Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1411 (2002) (arguing that *Kyllo* is insufficiently protective of privacy and that "[m]embers of our society should be constitutionally entitled to expect that government will refrain from *any* spying on the home — technological or otherwise — unless it can demonstrate good cause for doing so"); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1087 (2002) (arguing that Fourth Amendment doctrine does not protect privacy sufficiently against new technologies, and that Fourth Amendment law should create an "architecture of power" to maintain an appropriate balance of power among individuals, institutions, and the government in light of "the ever-increasing data flows of the Information Age"); David E. Steinberg, *Making Sense of Sense-Enhanced Searches*, 74 MINN. L. REV. 563, 629 (1990) (arguing that "[n]owhere is an appropriate application of the warrant clause more essential to protect the security promised by the fourth amendment" than in the case of sense-enhancing technologies); Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS., Spring 2002, at 125, 131 (arguing that Fourth Amendment protections should be expanded "by redefining privacy from the primarily cognitive to the primarily affective," and that "[p]rivacy in the information age is best conceived as the maintenance of metaphorical boundaries that define the contours of personal identity"); James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 438 (2002) (arguing that in order to protect privacy from the threat of new technologies, "[o]fficial exploitation of a scientific or technological device should be considered a Fourth Amendment search").

This theme is also a staple of law student note topics. For examples of law student notes reflecting this view culled from the law reviews published in the year 2003 alone, see, e.g., Melissa Arbus, Note, *A Legal U-Turn: The Rehnquist Court Changes Direction and Steers Back to the Privacy Norms of the Warren Era*, 89 VA. L. REV. 1729, 1730 (2003) ("In the furtherance of a free society . . . tools and technologies must be constrained by the individual

come first, legislatures a distant second. Justice Brandeis's famous dissent in *Olmstead v. United States*[8] provides the guiding light. Brandeis urged in 1928 that to protect our liberties as technology advances, "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[9] Seventy-five years later, modern commentators echo this approach with surprising uniformity. The view that the Fourth Amendment should be interpreted broadly in response to technological change has been embraced by leading theorists of law and technology such as Lawrence Lessig,[10] leading constitutional law figures such as Laurence Tribe,[11] and nearly everyone else who has written on the intersection of technology and criminal procedure.[12] Because of its broad support among leading commentators, I will label this approach the popular view of the Fourth Amendment and new technologies.

Although the popular view has been justified on many different grounds, most expressions of it tend to rest on one or more of three complementary premises. The first premise is doctrinal, the second is historical, and the third is functional. The doctrinal premise is that the courts should actively monitor technology's effects on privacy because

---

privacy rights embodied by the Fourth Amendment of the Constitution."); Rania M. Basha, Note, Kyllo v. United States: *The Fourth Amendment Triumphs Over Technology*, 41 BRANDEIS L.J. 939 (2003); Scott Byrd, Note, *Criminal Procedure: Searching High and Low for A Search in* Kyllo*: Justice Scalia Reaffirms Core Protections of the Fourth Amendment*, 56 OKLA. L. REV. 153 (2003); Jeffrey W. Childers, Comment, Kyllo v. United States*: A Temporary Reprieve from Technology-Enhanced Surveillance of the Home*, 81 N.C. L. REV. 728 (2003) (criticizing the Supreme Court for not protecting privacy enough through the Fourth Amendment in *Kyllo*); Courtney Dashiell, Comment, *Thermal Imaging: Creating 'Virtual' Space*, 34 U. TOL. L. REV. 351 (2003); Matthew Hector, Comment, *Privacy to be Patched in Later — An Examination of the Decline of Privacy Rights*, 36 J. MARSHALL L. REV. 985 (2003); Jessica T. Kobos, Note, Kyllo v. United States: *A Lukewarm Interpretation of the Fourth Amendment*, 64 MONT. L. REV. 519 (2003); Peter G. Madrian, Note, *Devil in the Details: Constitutional Problems Inherent in the Internet Surveillance Provisions of the USA PATRIOT Act of 2001*, 6 U. PITT. L. REV. 783 (2003); Rachel S. Martin, Note, *Watch What You Type: As the FBI Records Your Keystrokes, the Fourth Amendment Develops Carpal Tunnel Syndrome*, 40 AM. CRIM. L. REV. 1271 (2003).

8. 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting).

9. *Id.* at 478.

10. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 222-23 (1999) (contending that "there is an important space for [judicial] activism" in matters of Internet privacy and liberty, and that it is better to "err on the side of . . . [judicial] activism than on the side of . . . [judicial] passivity" in such cases).

11. *See* Laurence H. Tribe, The Constitution in Cyberspace, Keynote Address at the First Conference on Computers, Freedom, & Privacy (March 26, 1991) (transcript available at www.sjgames.com/SS/tribe.html) (arguing that the Fourth Amendment should apply broadly to new technologies so that mere "[a]ccidents of [t]echnology" do not determine constitutional protections, and claiming that minimalist Fourth Amendment decisions such as *Smith v. Maryland* "[s]adly . . . retreated" from the proper broad principles of Fourth Amendment protection).

12. See sources cited *supra* note 7.

Fourth Amendment doctrine demands it. The "reasonable expectation of privacy" test governs Fourth Amendment law,[13] and it is up to the courts to determine when an expectation of privacy is "reasonable."[14] As a result, the courts must update and redefine the Fourth Amendment as technology evolves, creating and recreating reasonable rules that effectively regulate law enforcement and protect privacy in new technologies. The historical premise suggests that the courts should play an active role in the regulation of new technologies because they have done so successfully in the past.[15] In particular, the Supreme Court's reversal of *Olmstead* and recognition of Fourth Amendment protections against government wiretapping in *Katz v. United States*[16] establish a precedent that supports future intervention. The third and final premise justifies a strong judicial role for reasons of institutional competence. Courts should take the lead crafting rules to protect privacy because courts are well-situated to regulate criminal investigations involving new technologies.[17] Taken together, these three arguments suggest that courts must, have, and should use the Fourth Amendment to provide the first line of defense against government invasions of privacy allowed by new technologies.

This article challenges the popular view of the role of the Fourth Amendment in new technologies. I will argue that the popular vision is based on a romantic but somewhat inaccurate view of Fourth Amendment doctrine, history, and function. Properly understood, considerations of doctrine, history, and function tend to counsel against an aggressive judicial role in the application of the Fourth Amendment to developing technologies. They teach that courts should place a thumb on the scale in favor of judicial caution when technology is in flux, and should consider allowing legislatures to provide the primary rules governing law enforcement investigations involving new technologies. While proponents of the popular view assume that the Fourth Amendment can play the same central role regulating government use of developing technologies that it has played in more traditional cases, there are sound reasons to treat developing technologies differently. These differences suggest that statutory rules rather than constitutional rules should provide the primary source of privacy protections regulating law-enforcement use of rapidly developing technologies. When technology is in flux, Fourth Amendment protections should remain relatively modest until the technology stabilizes.

---

13. Smith v. Maryland, 442 U.S. 735, 740 (1979) (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

14. *See* Section I *infra.*

15. *See* Section II *infra.*

16. 389 U.S. 347 (1967).

17. *See* Section III, *infra.*

This article aims to reorient current thinking about how the legal system should regulate criminal investigations involving new technologies. I want to nudge us away from thinking primarily in terms of the Fourth Amendment, and focus attention instead on legislative rules. I contend that the legislative branch rather than the judiciary should create the primary investigative rules when technology is changing. Contrary to the three premises underlying the popular view, legislative predominance in the face of developing technologies is consistent with current Fourth Amendment doctrine, accurately reflects historical practice, and is likely to continue in the future given the relative institutional competence of courts and legislatures. The institutional advantages of legislative rule making may eventually create a bifurcated privacy regime in which the governing law is primarily constitutional in most areas, but primarily statutory in areas of technological flux. Technological change may reveal the institutional limits of the modern enterprise of constitutional criminal procedure, exposing the need for statutory guidance when technology is changing rapidly. The implications for the field of criminal procedure are considerable. If criminal prosecutions involving new technologies continue to grow in number and importance, a basic understanding of criminal procedure rules may someday require as much knowledge of the United States Code as the United States Reports.

By arguing in favor of judicial caution, I don't wish to suggest that privacy in unimportant. To the contrary: privacy is one of our most cherished values, and rules that effectively regulate criminal investigations to prevent government abuse are essential to our traditions. At the same time, it is wrong to assume that courts necessarily generate more protective rules than legislatures. In recent decades, legislative privacy rules governing new technologies have proven roughly as privacy protective as, and quite often more protective than, parallel Fourth Amendment rules. Judicial deference has often invited Congressional regulation. As a result, the key question is less how much criminal procedure rules should protect privacy than whether we should look primarily to the courts or to Congress to generate those rules. I believe that we should look first to Congress when technology is changing rapidly. A renewed focus on the possibilities offered by legislative rules will enable the legal system to generate better rules — rules that are more nuanced, clear, and that optimize the critical balance between privacy and public safety more effectively when technology is in flux.

I will develop my argument in three parts. Each part challenges one of the premises supporting the popular view, and tells a cautionary tale about the limits of the Fourth Amendment when technology is in flux. Part I challenges the doctrinal premise that Fourth Amendment doctrine requires the courts to assume an active role that can

adequately protect privacy in new technologies. I argue that existing Fourth Amendment doctrine generally counsels in favor of caution in cases involving new technologies. The *Katz* "reasonable expectation of privacy" test has proven more a revolution on paper than in practice; *Katz* has had a surprisingly limited effect on the largely property-based contours of traditional Fourth Amendment law. As a result, courts rarely accept claims to Fourth Amendment protection in new technologies that do not involve interference with property rights, and have rejected broad claims to privacy in developing technologies with surprising consistency. The result is a critical gap between privacy rules the modern Fourth Amendment provides and privacy rules needed to effectively regulate government use of developing technologies.

Part II challenges the historical premise and its canonical example of wiretapping law. The popular view teaches that the Fourth Amendment constitutionalized the law and successfully tamed wiretapping practices. I argue that the impact of the Fourth Amendment on wiretapping law generally has been considerably overstated. Wiretapping law may be constitutional in theory thanks to *Berger v. New York*[18] and *Katz v. United States*,[19] but it remains largely statutory in fact. Courts interpreting the Fourth Amendment have generally deferred to statutory law in this area. In the decades since *Katz v. United States*, only a handful of judicial decisions have found that government wiretapping violated the Fourth Amendment. Nor is the dominance of statutory rules within wiretapping law necessarily unusual. The statutory Wiretap Act offers only one example of how criminal investigations in developing technologies have tended to be governed by statute. Although scholars tend to focus on the Fourth Amendment, the real privacy protection has more often derived from statutory law.

Part III challenges the functional premise of the popular vision. It argues that regulating developing technology through the Fourth Amendment poses significant difficulties for courts. The context of judicial decisionmaking presents few opportunities to clarify the law. Judicial decisions tend to incorporate outdated assumptions of technological practice, leading to rules that make little sense in the present or future. Courts also lack the information needed to understand how the specific technologies in cases before them fit into the broader spectrum of changing technologies, and cannot update rules quickly as technology shifts. Legislatures do not offer a panacea, but they do offer significant institutional advantages over courts. Legislatures can enact comprehensive rules based on expert input and can update them frequently as technology changes. As a result,

18. 388 U.S. 41 (1967).

19. 389 U.S. 347 (1967).

legislatures can generate more nuanced, balanced, and accurate privacy rules when technology is in flux. Courts should recognize their institutional limitations and remain cautious until the relevant technology and its applications stabilize.

I. THE FOURTH AMENDMENT AND THE DEFERENCE NORM IN NEW TECHNOLOGIES

Explanations of how the Fourth Amendment applies to developing technologies usually go something like this: the touchstone of the modern Fourth Amendment is the "reasonable expectation of privacy" test.[20] Police investigations that violate a reasonable expectation of privacy are unconstitutional unless the police obtain a warrant or some other exception applies. What counts as a "reasonable expectation of privacy" is very much up for grabs, however.[21] In this era of high-tech surveillance and the Internet, no one knows whether an expectation of privacy in a new technology is "reasonable."[22] Part of the problem is that the test is largely circular: a person has a reasonable expectation of privacy when the courts decide to protect it through the Fourth Amendment.[23] As a result, the law necessarily tasks the courts with fashioning Fourth Amendment protections in advanced technologies.[24] To decide the scope of Fourth

---

20. This test first appeared in Justice Harlan's concurrence in *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

21. *See, e.g.*, JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 60-61 (2001). *Cf.* CHARLES H. WHITEBREAD & CHRISTOPHER SLOBOGIN, CRIMINAL PROCEDURE: AN ANALYSIS OF CASES AND CONCEPTS § 4.03(f) at 116 (3d ed. 1993) (noting the Supreme Court's "mixed signals" on the question of how to determine a reasonable expectation of privacy).

22. *See* ROSEN, *supra* note 21, at 60-61; Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 401 (1997) (contending that the courts apply a multi-factored analysis to decide whether government conduct violates a reasonable expectation of privacy, and then concluding that "many of the factors that courts consider . . . are of dubious value"); A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 823-33 (1995) (discussing whether an expectation of privacy in encrypted communications is "reasonable").

23. *See, e.g.*, Michael Abramowicz, *Constitutional Circularity*, 49 UCLA L. REV. 1, 60-61 (2001) ("Fourth Amendment doctrine, moreover, is circular, for someone can have a reasonable expectation of privacy in an area if and only if the Court has held that a search in that area would be unreasonable."); ROSEN, *supra* note 21, at 60 ("Harlan's test was applauded as a victory for privacy, but it soon became clear that it was entirely circular.").

24. *See, e.g.*, 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT, § 2.1(d) at 391 (3d ed. 1996 & Supp. 2004) ("The criteria for reasonable expectations must be abstracted from the flow of life, and it is the judge's task to find and articulate those societal standards." (quoting Steven C. Douse, Note, *The Concept of Privacy and the Fourth Amendment*, 6 U. MICH. J.L. REFORM 154, 179-180 (1972))); *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV 349, 403 (1974) ("The ultimate question, plainly, is a value judgment . . . that the Fourth amendment inexorably requires the Court to make."); Rakas v. Illinois, 439 U.S. 128, 166 (1978) (White,

Amendment protection in a high-tech world, a judge must ruminate over the importance of privacy and the meaning of "reasonableness," and then make a normative assessment of what privacy protections should exist.

In this Part, I will argue that this popular understanding of the Fourth Amendment is generally at odds with how courts have applied the Fourth Amendment. Judges generally have declined to assume this active role because Fourth Amendment doctrine has remained heavily tied to real property concepts. In most contexts, whether an expectation of privacy is deemed reasonable can be answered by whether it is backed by what I will call a 'loose' version of real property law. Under these precedents, a "reasonable expectation of privacy" is not the same as the privacy that a reasonable person would expect. Instead, it acts as a term of art tied largely to traditional property law concepts. The difference often creates a wide gap between the privacy rules reasonable people want and the deferential rules that the Fourth Amendment provides. When technology is new or in flux, and its use may have privacy implications far removed from property law, Fourth Amendment rules alone will tend not to provide adequate privacy protections. Statutory protections are needed to protect privacy and regulate government uses of developing technologies.

A. *Property Law and the Fourth Amendment*

Scholars often describe Fourth Amendment law as unruly.[25] With so many decided cases and so few agreed-upon principles at work, trying to understand the Fourth Amendment is a bit like trying to put together a jigsaw puzzle with several incorrect pieces: no matter which way you try to assemble it, a few pieces won't fit.[26] In this section, I argue that despite this difficulty, a strong and underappreciated connection exists between the modern Fourth Amendment and real property law. Descriptively speaking, the basic contours of modern Fourth Amendment doctrine are largely keyed to property law. Although the phrase "reasonable expectation of privacy" sounds mystical, in most (though not all) cases, an expectation of privacy

---

J., dissenting) (contending that the reasonable expectation of privacy test is defined by the scope of privacy protection that is "essential to securing 'conditions favorable to the pursuit of happiness' " (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting))).

25. *See, e.g.*, Lloyd L. Weinreb, *Generalities of the Fourth Amendment*, 42 U. CHI. L. REV. 47, 49-50 (1974) (describing Fourth Amendment law as "a body of doctrine that is unstable and unconvincing"); Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1468-72 (1985) (describing the fourth amendment as "the Supreme Court's tarbaby: a mass of contradictions and obscurities").

26. *See id.*

becomes "reasonable" only when it is backed by a right to exclude borrowed from real property law.

Consider Fourth Amendment protections in the home. A homeowner has a reasonable expectation of privacy in his home: "At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[27] A renter of a house or apartment has a reasonable expectation of privacy in his home as well.[28] So long as the tenant complies with the rental contract that grants him the right to exclude others in exchange for rent money, he enjoys the full panoply of Fourth Amendment protections.[29] If the tenant's nonpayment of rent leads to eviction proceedings, however, the tenant loses his reasonable expectation of privacy in his home when he loses his right to be on the premises according to state property law.[30] Similar rules apply to Fourth Amendment rights in hotel rooms and storage lockers.[31] A person who rents out a hotel room or storage locker enjoys Fourth Amendment rights in the rented space so long as he complies with the rental contract.[32] When he ceases to pay rent and no longer enjoys a legal right to exclude others from the space, however, his Fourth Amendment protections in the space quickly disappear.[33]

---

27. Silverman v. United States, 365 U.S. 505, 511 (1961).

28. *See* Chapman v. United States, 365 U.S. 610 (1961) (holding that the Fourth Amendment protects a leaseholder from a search by the police consented to by the landowner).

29. *See* United States v. Showalter, 858 F.2d 149, 151 (3d Cir. 1988) (stating that defendants who had "resided on the property under a lease agreement with the owner . . . had a reasonable expectation of privacy in the premises"). *See also* Minnesota v. Carter, 525 U.S. 83, 95-96 (1998) (Scalia, J., concurring).

> Of course this is not to say that the Fourth Amendment protects only the Lord of the Manor who holds his estate in fee simple. People call a house "their" home when legal title is in the bank, when they rent it, and even when they merely occupy it rent free — so long as they actually live there.

Id.

30. *See, e.g.*, Simpson v. Saroff, 741 F. Supp. 1073, 1078 (S.D.N.Y. 1990) (citing cases); United States v. Botelho, 360 F. Supp. 620, 624 (D. Haw. 1973) (holding that whether a tenant retained Fourth Amendment rights in a rented apartment depended on whether he had a right to occupy the premises under state property law).

31. *See, e.g.*, United States v. Nerber, 222 F.3d 597, 600 n.2 (9th Cir. 2000) ("For Fourth Amendment purposes, a hotel room is treated essentially the same, if not exactly the same, as a home.").

32. *See, e.g.*, Stoner v. California, 376 U.S. 483, 489 (1964) (upholding Fourth Amendment rights in a rented hotel room); United States v. Karo, 468 U.S. 705, 721 n.6 (1984) (noting that defendants ordinarily retain Fourth Amendment rights in their storage lockers).

33. *See* United States v. Dorais, 241 F.3d 1124, 1128 (9th Cir. 2001) (stating that "a defendant has *no* reasonable expectation of privacy in a hotel room when the rental period has expired and the hotel has taken affirmative steps to repossess the room"); United States v. Poulsen 41 F.3d 1330, 1337 (9th Cir. 1994) (holding that defendant's nonpayment of rent

The Fourth Amendment rights track the right to exclude others under state property law.[34]

The Fourth Amendment rights of visitors to homes follow similar principles. The key question is whether the homeowner or his agent has explicitly or implicitly delegated to the visitor the homeowner's right to exclude others from the property. For example, if the visitor is living at the home with the owner's consent, the visitor enjoys full Fourth Amendment protections.[35] The same goes for an overnight guest who was invited to stay at the home by the homeowner.[36] If the visitor is not staying on the property with the homeowner's consent or otherwise has no previous relationship with the owner, however, he cannot establish a reasonable expectation of privacy there.[37] Thus, a squatter who trespasses on the land of another and lives there without authorization cannot establish a reasonable expectation of privacy in the land.[38] Because the squatter has "no legal right to occupy the land,"[39] he cannot earn Fourth Amendment protections even in his home.

Nor are the rules governing homes unique. The same principles govern Fourth Amendment protection in automobiles. The owner of a car enjoys Fourth Amendment protection in the car, as does a guest who has been allowed to use the car by the owner.[40] A person who is

---

for storage locker extinguished his Fourth Amendment rights in the locker when it ended defendant's right to exclude others from accessing the locker under state property law).

34. Rakas v. Illinois, 439 U.S. 128, 143-44 n.12 (1978).

> One of the main rights attaching to property is the right to exclude others, see W. Blackstone, Commentaries, Book 2, ch. 1, and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude.

Id.

35. *See* Bumper v. North Carolina, 391 U.S. 543, 548 n.11 (1968) (holding that an unreasonable search of a grandmother's house violated her resident grandson's Fourth Amendment rights).

36. *See* Minnesota v. Olson, 495 U.S. 91, 98-99 (1990) (concluding that an authorized overnight guest has a reasonable expectation of privacy in the home he is visiting).

37. *See* Minnesota v. Carter, 525 U.S. 83, 91 (1998) (holding that two men visiting an apartment to package cocaine did not have a reasonable expectation of privacy in the apartment given "the purely commercial nature of the transaction engaged in here, the relatively short period of time on the premises, and the lack of any previous connection between respondents and the householder"). *Cf.* Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) (noting that a burglar who has entered a home to commit a crime cannot have a reasonable expectation of privacy there).

38. *See* Amezquita v. Colon, 518 F.2d 8, 12 (1st Cir. 1975) (holding that squatters residing on government land did not have a reasonable expectation of privacy in their homes).

39. *Id.*

40. *See* United States v. Baker 221 F.3d 438, 442 (3d Cir. 2000) (holding that a defendant who drove a car with the permission of the owner had a reasonable expectation of privacy in the car); United States v. Garcia, 897 F.2d 1413, 1418 (7th Cir. 1990) (same); United States v. Muhammad, 58 F.3d 353, 355 (8th Cir. 1995) ("Both parties agree that the defendant must

found driving a stolen car, however, does not enjoy Fourth Amendment protection within it.[41] The same rules apply to rental cars. Whether a person has Fourth Amendment rights in a rental car depends upon whether his name appears on the rental contract: if his name does appear on the contract, he is a legitimate user with Fourth Amendment rights.[42] If his name does not appear, he does not have the owner's permission to drive the car and will have no Fourth Amendment rights in the car.[43]

The same property-based rules apply to Fourth Amendment rights in "closed containers,"[44] a category that the courts have used to describe everything from sealed letters[45] and boxes[46] to computer files.[47] The owner of a closed container ordinarily has a reasonable expectation of privacy in its contents.[48] This is true regardless of whether the container is locked securely or merely covered by a flimsy opaque cover.[49] If the owner abandons the container, relinquishing his property right, a government search of the container cannot violate his Fourth Amendment rights.[50] Similarly, an individual normally will not retain a reasonable expectation of privacy in the contents of a stolen container because he lacks a property interest in the container.[51]

---

present at least some evidence of consent or permission from the lawful owner/renter to give rise to an objectively reasonable expectation of privacy.").

41. *See* United States v. Sholola, 124 F.3d 803, 815 n.14 (7th Cir. 1997) (citing *Garcia*, 897 F.2d at 1417); United States v. Tropiano, 50 F.3d 157, 161 (2d Cir. 1995) (citing cases).

42. *See* United States v. Wellons, 32 F.3d 117, 119 (4th Cir. 1994) (citing cases).

43. *See id.*

44. United States v. Ross, 456 U.S. 798, 822 (1982).

45. Walter v. United States 447 U.S. 649, 654-55 n.5 (1980) (quoting Ex Parte Jackson, 96 U.S. 727, 732 (1878)).

46. *Ross*, 456 U.S. at 822.

47. Trulock v. Freeh, 275 F.3d 391, 410 (4th Cir. 2001) (Michael, J., concurring in part and dissenting in part) ("Courts have not hesitated to apply established Fourth Amendment principles to computers and computer files, often drawing analogies between computers and physical storage units such as file cabinets and closed containers." (citing cases)).

48. *Ross*, 456 U.S. at 822.

49. *See id.*

> For just as the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion, so also may a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case.

50. *See* California v. Greenwood, 486 U.S. 35, 39 (1988) (concluding that defendants did not retain a reasonable expectation of privacy in opaque containers of garbage that they had left at the edge of their property with the purpose to convey to garbage collectors).

51. *See, e.g.*, United States v. Lyons, 992 F.2d 1029, 1031 (10th Cir. 1993) (concluding that a defendant had no Fourth Amendment rights in the contents of stolen computer hard drives) ("Because expectations of privacy derive in part from the right to exclude others from the property in question, lawful possession is an important consideration in

Even the rights of an owner are not absolute under the Fourth Amendment.[52] The courts have sanctioned a wide range of invasive warrantless surveillance techniques that threaten privacy but not property. So long as the surveillance does not invade the individual's right to exclude others — the very essence of the property right[53] — the surveillance generally does not violate his reasonable expectation of privacy. For example, the police can invade the privacy of a homeowner by standing in the public street and peeking into his home through a window,[54] and can use a flashlight that illuminates the inside.[55] The police can rent helicopters, fly high enough to reach public airspace where property rights no longer govern, and then take photographs of the home.[56] Police informants can also assume undercover identities and trick the homeowner into letting them inside while wearing a recording device,[57] or else convince another person who has common authority over the home to consent to a search.[58] All of these techniques are invasive. All of them appear to violate the homeowner's "right to be let alone."[59] None of these techniques violate the homeowner's property rights, however, and under existing law none of them constitute a Fourth Amendment search.

---

determining whether a defendant had a legitimate expectation of privacy in the area searched, i.e. the hard disks.").

52. *See* California v. Ciarolo, 476 U.S. 207, 213 (1986) (noting that the fact that property is considered within the curtilage of the home "does not itself bar all police observation").

53. *See* Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 730 (1998) (noting that the essence of a property right is the right to exclude others); Felix S. Cohen, *Dialogue on Private Property*, 9 RUTGERS L. REV. 357, 374 (1954) (same).

54. *See, e.g.*, Kyllo v. United States, 121 S. Ct. 2038, 2042 (2001) (noting that under modern Fourth Amendment law, "the lawfulness of warrantless visual surveillance of a home has still been preserved."); *Ciarolo*, 476 U.S. at 213 ("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."). *See also* Texas v. Brown, 460 U.S. 730, 740 (1983) (holding that police can peer through a window inside a defendant's automobile without implicating the Fourth Amendment).

55. *See* United States v. Dunn, 480 U.S. 294, 305 (1987) (holding that law enforcement officers' use of a flashlight to illuminate the inside of a barn does "not transform their observations into an unreasonable search within the meaning of [the] Fourth Amendment.").

56. *See* Florida v. Riley, 488 U.S. 445, 451 (1989) (plurality) (concluding that warrantless aerial surveillance from public airspace does not violate the Fourth Amendment); *see id.* at 452 (O'Connor, J., concurring).

57. United States v. White, 401 U.S. 745, 753-54 (1971).

58. *See* United States v. Matlock, 415 U.S. 164, 171 (1974).

> [W]hen the prosecution seeks to justify a warrantless search by proof of voluntary consent, it is not limited to proof that consent was given by the defendant, but may show that permission to search was obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected.

Id.

59. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

Moving beyond searches, the Fourth Amendment rules governing seizures are explicitly property-based. Whereas a search occurs when government action violates a defendant's reasonable expectation of privacy, a seizure occurs only when the government action causes a "meaningful interference with an individual's possessory interests in . . . property."[60] This standard allows the government to photocopy a defendant's papers[61] or make an electronic copy of his computer files[62] without that copying constituting a Fourth Amendment seizure. Because the copying does not dispossess the owner of the original property, copying does not seize anything according to current Fourth Amendment doctrine.[63]

Of course, I cannot claim that *all* Fourth Amendment decisions track real property law. Important exceptions exist. For example, the Supreme Court has tended to ignore property principles when evaluating Fourth Amendment restrictions on bodily outputs. The Court has held that the Fourth Amendment does not protect handwriting samples[64] or the human voice,[65] not because they are not property but because they are not sufficiently private.[66] Similarly, the Court has enacted *sui generis* rules for how the Fourth Amendment applies to government workplaces. In *O'Connor v. Ortega*,[67] the Court held that a government employee will enjoy a reasonable expectation

60. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

61. *See* United States v. Thomas, 613 F.2d 787, 793 (10th Cir. 1980) (holding that the FBI did not "seize" defendant's written and photographic materials when they photocopied the materials, because the FBI did not affect the owner's possession of the originals).

62. *See* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001).

> [T]he agents' act of copying the data on the . . . computers was not a seizure under the Fourth Amendment because it did not interfere with Defendant's or anyone else's possessory interest in the data. The data remained intact and unaltered. It remained accessible to Defendant and any co-conspirators or partners with whom he had shared access. The copying of the data had absolutely no impact on his possessory rights.

Id.

63. *But see* United States v. Freitas, 800 F.2d 1451, 1455 (9th Cir. 1986) (concluding that Federal Rule of Criminal Procedure 41 allows the police to obtain a warrant authorizing them to view a defendant's property but not seize any tangible property, on the ground that the Rule allows the police to obtain a warrant to seize property, and viewing the property constitutes a seizure of "information regarding the 'status of the [property to be viewed]' ").

64. United States v. Mara, 410 U.S. 19, 21 (1973).

65. United States v. Dionisio, 410 U.S. 1, 14 (1973).

66. *See* Mara, 410 U.S. at 21 ("Handwriting, like speech, is repeatedly shown to the public, and there is no more expectation of privacy in the physical characteristics of a person's script than there is in the tone of his voice."); Dionisio, 410 U.S. at 14 ("The physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. Like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear.").

67. 480 U.S. 709 (1987) (plurality opinion).

of privacy only if under "actual office practices and procedures"[68] the employee's workspace is not "open to fellow employees or to the public."[69] Government employee privacy hinges not on the usual right to exclude, but rather on whether it is reasonable in context for employees to expect that others will not enter their space.[70] Another possible exception is the 'open fields' doctrine, which allows the government to trespass onto uncultivated land belonging to the defendant so long as they do not approach areas immediately adjacent to the home.[71] Despite these examples, I think that my softer point survives. Although no one theory explains the entire body of Fourth Amendment doctrine, property law provides a surprisingly accurate guide.

B. Katz v. United States *and the Property-Based View*

How can this property-based Fourth Amendment be squared with the leading case in Fourth Amendment law, *Katz v. United States*?[72] Fourth Amendment scholarship generally teaches that under *Katz* the modern Fourth Amendment protects privacy, not property,[73] and that it protects privacy primarily by answering the normative question of when an expectation of privacy should be deemed constitutionally "reasonable."[74] This section argues that the mainstream academic

---

68. *Id.* at 717.

69. *Id.* at 718.

70. *See id.* at 717; Rossi v. Town of Pelham, 35 F. Supp. 2d 58, 63-64 (D.N.H. 1997). This standard differs significantly from the standard analysis applied in private workplaces. Private-sector employees will generally retain an expectation of privacy in their work space unless that space is "open to the world at large." United States v. Lyons, 706 F.2d 321, 326 (D.C. Cir. 1983). Thus, if two private-sector employees share an office, the sharing of the office does not eliminate Fourth Amendment protection. Mancusi v. DeForte, 392 U.S. 364, 369 (1968). In contrast, sharing an office will normally eliminate Fourth Amendment protection for a government employee. *See, e.g.*, Sheppard v. Beerman, 18 F.3d 147, 152 (2d Cir. 1994) (holding that judge's search through his law clerk's desk and file cabinets did not violate the clerk's reasonable expectation of privacy because of the clerk's close working relationship with the judge). *See also* O'Connor, 480 U.S. at 730-31 (Scalia, J., concurring) (noting the difference between the expectation-of-privacy analysis offered by the O'Connor plurality and that traditionally applied in private workplace searches).

71. *See* Oliver v. United States, 466 U.S. 170, 183-84 (1984) ("[I]n the case of open fields, the general rights of property protected by the common law of trespass have little or no relevance to the applicability of the Fourth Amendment."). An "open field" is "any unoccupied or undeveloped area outside of the curtilage," or one which is too far, too exposed, and not intimate enough to be protected like the house. *See* United States v. Dunn, 480 U.S. 294, 304 (1987).

72. 389 U.S. 347 (1967).

73. *See, e.g.*, JEROLD H. ISRAEL & WAYNE R. LAFAVE, CRIMINAL PROCEDURE IN A NUTSHELL 60 (5th ed., 1993) ("Th[e] property approach was rejected in *Katz v. U.S.* (1967), in favor of a privacy approach.").

74. *See* ANDREW E. TASLITZ & MARGARET L. PARIS, CONSTITUTIONAL CRIMINAL PROCEDURE 95 (1997) ("The *Katz* test demands that the courts define privacy and determine when it can be reasonably protected."). *See also* supra notes 24-25 and

understanding has often overlooked the continuing influence of property concepts because it has tended to misconstrue cases that rejected strict common law property rules as Fourth Amendment guides. While existing scholarship often interprets the shift as a wholesale rejection of property-based principles in Fourth Amendment law, it is better understood as a shift of degree from common law rules to the looser property-based approach that currently governs. Viewed in this light, the *Katz* "reasonable expectation of privacy" test has more bark than bite and has not substantially changed the basic property-based contours of Fourth Amendment law.

It is generally agreed that before the 1960s, the Fourth Amendment was focused on the protection of property rights against government interference.[75] The Fourth Amendment was enacted largely in response to English cases such as *Entick v. Carrington*,[76] in which Lord Camden had declared that "our law holds the property of every man so sacred, that no man can set his foot upon his neighbor's close without his leave; if he does he is a trespasser . . . . [and] if he will tread upon his neighbor's ground, he must justify it by law."[77] In light of this history, early courts interpreted the Fourth Amendment as a claim against government interference with property rights, and in particular, rights against trespass.

The classic case illustrating the property-based Fourth Amendment is *Olmstead v. United States*[78] from 1928. *Olmstead* was the first wiretapping case decided by the Supreme Court. Government agents climbed up telephone poles on public streets outside Roy Olmstead's home and offices and tapped telephone lines running to and from them.[79] The Court held that the wiretapping was not a "search" or "seizure" under the Fourth Amendment.[80] Chief Justice

---

accompanying text. A few scholars have noticed the continuing vitality of real property law to the Fourth Amendment. *See, e.g.*, Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 316-20 (1988) (noting that Fourth Amendment rules in practice are often tied to property rights); Daniel B. Yeager, *Search, Seizure and the Positive Law: Expectations of Privacy Outside the Fourth Amendment*, 84 J. CRIM. L. & CRIMINOLOGY 249, 251 (1993). These scholars are in a distinct minority, however.

75. *See, e.g.*, Warden v. Hayden, 387 U.S. 294, 303-06 (1967).

76. 95 Eng. Rep. 807 (K.B. 1765).

77. *Id.* at 817.

78. 277 U.S. 438 (1928).

79. *See id.* at 457. As the majority opinion notes, Olmstead's criminal operation was "a conspiracy of amazing magnitude," and the wiretapping was similarly widespread. *See id.* at 455. For an informative history of the *Olmstead* case, see WALTER F. MURPHY, WIRETAPPING ON TRIAL, A CASE STUDY IN THE JUDICIAL PROCESS (1965).

80. *Olmstead*, 277 U.S. at 466 ("We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.").

Taft reasoned that the wiretap was not a search because it did not violate Olmstead's property rights: in the language of the Court, "[t]here was no entry of the houses or offices of the defendants."[81] Justice Brandeis dissented, offering a dramatically different approach to the Fourth Amendment. According to Brandeis, "the physical location" of the telephone wires was "immaterial."[82] Privacy mattered, not property: "[E]very unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[83] Despite Justice Brandeis's eloquence, his approach to the Fourth Amendment was endorsed only by two other Justices.[84]

How to interpret what happened in the 1960s is the real crux of the matter. Existing scholarship generally teaches that the Supreme Court rejected the property-based approach of *Olmstead* in 1967 when it decided *Katz v. United States*.[85] According to this theory, *Katz* rejected the property-based view and replaced it with a "reasonable expectation of privacy" test that echoes Justice Brandeis's dissent in *Olmstead*.[86] Under this interpretation, the "reasonable expectation of privacy" test has a normative component a la Justice Brandeis. As Professor Amsterdam wrote in his seminal and oft-quoted 1974 article, the question of when an expectation of privacy is reasonable "is a value judgment" that looks to whether the government practice is

---

81. *Id.* at 464.

82. *Id.* at 479 (Brandeis, J., dissenting).

83. *Id.* at 478.

84. Four Justices dissented in *Olmstead*: Justices Holmes, Brandeis, Butler and Stone. Each wrote their own dissents. Justice Stone agreed explicitly with Justice Brandeis's approach: Justice Butler did so implicitly. Justice Holmes, however, did not agree with Brandeis's approach to the Fourth Amendment, and instead wished to overturn the conviction on the theory that evidence collected in violation of state laws (here state wiretapping laws) should be suppressed. *See Olmstead*, 277 U.S. at 469 (Holmes, J., dissenting) ("While I do not deny it I am not prepared to [join Justice Brandeis and] say that the penumbra of the Fourth and Fifth Amendments covers the defendant . . . .").

85. *See, e.g.*, Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 248 (1993) ("At the beginning of the decade, the Court hinted that it was ready to jettison the property-privacy nexus, but the doctrine survived until the Court's 1967 decision in *Katz v. United States*."); ISRAEL & LAFAVE, *supra* note 73, at 60 ("Th[e] property approach was rejected in *Katz v. U.S.* (1967), in favor of a privacy approach.").

86. *See, e.g.*, LESSIG, *supra* note 10, at 116 ("It took forty years for the Supreme Court to embrace Brandeis's picture of the Fourth Amendment . . . [in] *Katz v. United States*."); Scott E. Sundby, *Everyman's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1756 (1994) ("Justice Brandeis's view of the Fourth Amendment became accepted by the Court in a later eavesdropping case, *Katz v. United States*."); Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 199 (1999) ("Almost forty years later, the Court adopted Justice Brandeis' reasoning in *Katz v. United States*."); Anjali Singhal, *The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography*, 7 STAN. L. & POL'Y REV. 189, 192 (1996) ("Brandeis' dissent was adopted by a majority forty years later in *Katz v. United States*.").

"[c]onsistent with the aims of a free and open society."[87] This approach envisions *Katz* as a test that embraces whatever rules are needed to protect privacy against new technologies.

As a description of existing judicial practice, however, this popular view is misleading. *Katz* did not adopt Brandeis's approach in *Olmstead*. Brandeis's dissent receives no mention in any of the opinions filed in the *Katz* case. Ironically, the only mention of Brandeis occurs when the majority rejects the view that the Fourth Amendment protects the right to be let alone that Brandeis described in his famous law review article *The Right To Privacy*.[88] More broadly, *Katz* can plausibly be read (and implicitly has been read by many courts) not as rejecting the existing property view of the Fourth Amendment, but as merely reemphasizing the Court's turn to a looser version of the property focused approach first introduced in 1960 in *Jones v. United States*.[89] To understand existing judicial practice, I think it helps to start with *Jones*, and see the later doctrine articulated in *Katz* as a reflection of the loose property-based view from *Jones*.

Cecil Jones was arrested inside an apartment in Washington, DC, in possession of narcotics and narcotics paraphernalia. The apartment belonged to Jones's friend Evans, who had given Jones the key and allowed him to stay at the apartment for a few nights while Evans was out of town. Following Jones's arrest, Jones moved to suppress the evidence found in Evans's apartment. The District Court rejected Jones's claim on the ground that Jones was not "a person aggrieved" by the search who could challenge its legality under the Federal Rules of Criminal Procedure.[90] Both then and now, this inquiry has been considered analogous to asking whether the defendant had Fourth Amendment standing.[91] The District Court's decision reflected the

---

87. Amsterdam, *supra* note 24, at 403. *See also* Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 124 (2002) (arguing that the "reasonable expectation of privacy" test forces "[d]ecisions . . . [to] rest on normative choices.").

88. *See Katz*, 389 U.S. at 350 (citing Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)). The Court in *Katz* rejected the broad Brandeisian formulation with the following analysis:

> [T]he Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion. But the protection of a person's *general* right to privacy — his right to be let alone by other people — is, like the protection of his property and of his very life, left largely to the law of the individual States.

Katz, 389 U.S. at 350-51.

89. 362 U.S. 257 (1960).

90. *See* Jones v. United States, 262 F.2d 234, 237 (D.C. Cir. 1958) (discussing the District Court's opinion).

91. *See* Rakas v. Illinois, 439 U.S. 128, 133 (1978).

common law property distinctions that the lower courts (although never the Supreme Court) had followed to determine standing to challenge warrants. In those decisions, the courts had held that "ownership" established standing, as did "dominion" and the status of being a "lessee or licensee." In contrast, "guests," "invitees," and employees who held "occupancy" but not "possession" lacked a sufficient property interest to challenge illegal searches.[92] Because Jones was merely a guest, he lacked standing to challenge the search of his friend's apartment.

The Supreme Court took a different view. Writing for the Court, Justice Frankfurter argued that arcane common law property rules should not resolve the standing inquiry:

> [I]t it is unnecessary and ill-advised to import into the law surrounding the constitutional right to be free from unreasonable searches and seizures subtle distinctions, developed and refined by the common law in evolving the body of private properly law which, more than almost any other branch of law, has been shaped by distinctions whose validity is largely historical.... Distinctions such as those between 'lessee,' 'licensee,' 'invitee' and 'guest,' often only of gossamer strength, ought not to be determinative in fashioning procedures ultimately referable to constitutional safeguards.[93]

In place of common law property distinctions, the Court adopted a looser standard that focused on whether the defendant's presence was "legitimate" or "wrongful":

> No just interest of the Government in the effective and rigorous enforcement of the criminal law will be hampered by recognizing that anyone legitimately on premises where a search occurs may challenge its legality by way of a motion to suppress, when its fruits are proposed to be used against him. This would of course not avail those who, by virtue of their wrongful presence, cannot invoke the privacy of the premises searched.[94]

Jones does not reject property as a guide to determine standing to challenge search warrants. Rather, *Jones* suggests that when using property as a guide, a broader conception of property should govern, not the arcane and hypertechnical distinctions of common law property rules. As the Court later expressed in a 1978 case, *Rakas v. Illinois*,[95] while "*arcane distinctions* developed in property... ought not to control"[96] the Fourth Amendment inquiry, "property *concepts*

92. The cases are collected in *Jones*, 362 U.S. at 265-66.

93. *Jones*, 362 U.S. at 266 (internal citations omitted).

94. *Id.* at 267.

95. 439 U.S. 128 (1978).

96. *Id.* at 143 (emphasis added).

in determining the presence or absence of the privacy interests protected by [the Fourth] Amendment"[97] are still useful.

This brings us back to *Katz*. Today, *Katz* is canonized as a landmark decision that dramatically changed Fourth Amendment law. Professor Amsterdam called it a "watershed in fourth amendment jurisprudence."[98] Others have described it as "revolutionary."[99] Yet a close examination of *Katz* suggests a plausible contrary reading: *Katz* did not revolutionize Fourth Amendment law, but merely reemphasized the loose property-based approach announced in *Jones*. Indeed, while Justice Harlan's concurrence in *Katz* did introduce the "reasonable expectation of privacy test," that doctrinal formulation was apparently meant merely to articulate the legal standard that the Court had been tacitly applying in past cases — cases such as *Jones v. United States*.

Katz began with an investigation into an illegal betting scheme. The FBI taped a microphone to the roof of a public phone booth used every morning by a suspect named Charles Katz.[100] The microphone was connected by a wire to an FBI listening post.[101] When Katz placed calls from the phone booth, the FBI turned on the microphone. The government played the recordings of Katz placing his bets at trial.[102] The microphone did not actually wiretap the telephone line: it merely recorded Katz's end of the conversations, picking up what an eavesdropper might have heard had he stood near the booth when Katz used the phone.[103] The lower courts approved this warrantless surveillance without difficulty.[104] Applying pre-*Jones* precedents that had adopted a strict property-based view of the Fourth Amendment, lower courts held that this monitoring did not violate Katz's Fourth Amendment rights because it did not physically trespass into the phone booth.[105]

---

97. *Id.* at 143-44 n.12 (emphasis added).

98. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 382 (1974).

99. James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 649 (1985) (referring to "[t]he *Katz* Revolution"); Richard G. Wilkins, *Defining the 'Reasonable Expectation of Privacy': An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077, 1087 (1987) ("*Katz* revolutionized fourth amendment search analysis.").

100. *See* Katz v. United States, 369 F.2d 130, 131 (9th Cir. 1966). The Supreme Court described the microphone as an "electronic listening and recording device," *see Katz*, 389 U.S. at 348, but the Ninth Circuit opinion describes the device simply as a microphone.

101. *See Katz*, 369 F.2d at 131.

102. *See Katz*, 389 U.S. at 354 n.14.

103. *See id.*

104. *See Katz*, 369 F.2d at 134.

105. *See Katz*, 369 F.2d at 134.

The Supreme Court took a different view. Echoing *Jones*, the Court stated that technical notions of common law trespass no longer governed the Fourth Amendment inquiry. The "narrow view"[106] of property rights simply could "no longer be regarded as controlling."[107] The Court suggested that a broader approach applied that allowed "a person in a telephone booth [to] rely upon the protection of the Fourth Amendment."[108] Writing for the majority, Justice Stewart did not define the contours of this broader approach. Instead, Justice Stewart made the conclusory statement that, "One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[109]

Exactly *why* the user of the phone booth was constitutionally entitled to his privacy was left to the reader's imagination. The Court did state that "the Fourth Amendment protects people rather than places,"[110] but this memorable line was apparently more a response to the litigants' briefs than a new principle of Fourth Amendment law.[111]

---

106. *Katz*, 389 U.S. at 353.

107. *Id.*

108. *Id.* at 352.

109. *Id.*

110. *See id.* at 347.

111. Katz's brief had argued to the Court that the very nature of phone booths triggered Fourth Amendment protection; any time the government wanted to collect information from a phone booth, Katz contended, the government needed a warrant. Katz's brief framed "the crucial inquiry as . . . whether a public telephone booth is a constitutionally protected area." Brief for Petitioner at 12, Katz v. United States, 389 U.S. 347 (1967). Katz argued that the Court's past Fourth Amendment decisions had recognized that business offices, stores, hotel rooms, automobiles, and taxicabs were all constitutionally protected areas, such that "it would be unreasonable to suggest that any less protection should be afforded to the user of a closed door public telephone booth." *Id.* at 14. The Solicitor General's brief for the United States offered a mirror image at this argument: it claimed that the very nature of phone booths meant that Fourth Amendment protection could never exist in a phone booth. The Government's brief argued that "[a] row of public telephone booths, . . . is not significantly different" from an open field or a public street because phone booths are exposed to the public, and someone speaking in a phone booth can be both readily overhead from an adjoining booth and also viewed through the glass. Brief for the United States at 15-16. This focus on a phone booth as a place followed from a sentence in an earlier case, *Silverman v. United States*, 365 U.S. 505, 512 (1961). which had suggested that Fourth Amendment protections hinged on whether the place searched was a "constitutionally protected area."

But the parties' abstraction of this inquiry made little sense under any conception of the Fourth Amendment. Even under the strict common law property view rejected in *Jones*, the Fourth Amendment protected a *person's* rights, namely their right to exclude others from their property. Consider the context in which the Court used its "people, not places" formulation. After reciting the questions presented by the petitioner, the Court "decline[d] to adopt this formulation of the issues," noting that "the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.' ":

> Because of the misleading way the issues have been formulated, the parties have attached great significance to the characterization of the telephone booth from which the petitioner placed his calls. The petitioner has strenuously argued that the booth was a "constitutionally protected area." The Government has maintained with equal vigor that it was not. But this

Only Justice Harlan articulated a coherent rationale for the Court's conclusion. In his famous concurrence, Harlan noted that the post-*Jones* Court had properly rejected a strict common law approach to the Fourth Amendment because it had proved to be "bad physics as well as bad law."[112] Justice Harlan argued that the Court's recent cases had focused instead on whether a defendant's expectation of privacy was reasonable under the circumstances.[113] Harlan did not explain what made an expectation of privacy "reasonable," but he apparently saw his "reasonable expectation of privacy" framework as a restatement of existing law; Harlan described the test as "my understanding of the rule that has emerged from prior decisions."[114] Applying this standard led Harlan to conclude that the monitoring violated Katz's Fourth Amendment rights. The "critical" fact was the relationship that Katz had established when he occupied the phone booth, shut the door behind him, and "pa[id] the toll that permit[ted] him to place a call."[115] At that point, the phone booth became a "temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable."[116]

Katz is a Rorschach test. Its vague language can support a narrow or broad reading equally well. But for my purpose here, note that *Katz* is correctly decided from the standpoint of the loose property-based approach applied in *Jones*. Charles Katz became entitled to Fourth Amendment protection when he "pa[id] the toll that permit[ted] him to place a call,"[117] because at that point he became a legitimate user of the phone booth. In effect, Katz rented out the booth for the "momentary"[118] period of his call much like a hotel guest rents out a hotel room for the night.[119] Like the hotel guest gaining Fourth

---

effort to decide whether or not a given "area," viewed in the abstract, is "constitutionally protected" deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places.

Katz, 389 U.S. at 350-51.

112. *Id.* at 362 (Harlan, J., concurring).

113. *See id.* at 361. ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' ").

114. Justice Harlan then interpreted the majority opinion in *Katz* as holding "only" that telephone booths receive Fourth Amendment protection, that electronic intrusions could violate the Fourth Amendment, and that warrantless searches were presumptively unreasonable. *See id.* at 361.

115. *Id.* at 361.

116. *Id.*

117. *Id.* at 352.

118. *Id.* at 361.

119. *See supra* notes 34-36, and accompanying text.

Amendment rights in the hotel room during his stay, Katz acquired the owner's privacy rights in the phone booth during the period of his phone call.

From this perspective, the FBI's surveillance violated the Fourth Amendment because it interfered with Katz's "momentary" property rights, and in particular his right to exclude others. The FBI had installed a microphone on the property Katz had rented out and connected the microphone by wire to an FBI listening post. In a Fifth Amendment case, *Loretto v. Teleprompter Manhattan CATV*,[120] the Supreme Court later found a similar installation to be a direct taking of private property requiring due compensation to the property owner.[121] In *Loretto*, the owner of an apartment building challenged the state-sanctioned installation of cable television boxes and connecting wires on the outside walls and roof of her building. Even though the installed devices were fairly small, used previously unused space,[122] and did not trespass into the inside of the building, the Court classified the installation as a "permanent physical occupation" of the owner's private property, "perhaps the most serious form of invasion of an owner's property interests."[123] The same applies to *Katz* in the context of the Fourth Amendment. In *Katz*, the government installed a device on the property Katz had rented out, and used that invasion of his property interest to collect evidence against him. Charles Katz was entitled to the suppression of the fruits derived from the government's invasion of his property interest no less than Loretto was entitled to just compensation for the government's invasion of her property interest. By entering the phone booth and paying for a call, Charles Katz bought a temporary right to exclude others from the phone booth that was protected by the Fourth Amendment.[124]

Is this the best interpretation of *Katz*? Not necessarily. Is it the only interpretation? Clearly not. Subsequent dissents by Justice Harlan suggest that he may have had a broader, more amorphous concept in mind.[125] At the same time, *Katz's* consistency with the property-based approach may help explain why the decision failed to

---

120. 458 U.S. 419 (1982).

121. *See id.* at 438.

122. *See id.* at 438 n.16.

123. *See id.* at 435.

124. *Cf.* Sklansky, *supra* note 7, at 158 ("[E]ven the central holding of *Katz* starts to look trivial if one ties it, as Harlan did, to an analogy between telephone booths and homes.").

125. Just a year after *Katz* in *Alderman v. United States*, 394 U.S. 165 (1969), Justice Harlan complained that the Court was not being true to *Katz* by adopting a property-based view of who has standing to challenge wiretapping practices. Harlan argued that only those who had their conversations tapped had standing; the majority opinion concluded that the homeowner had standing as well due to his ownership interest in the home where the telephone was located. *See id.* at 193-95 (Harlan, J., concurring in part and dissenting in part). *See also* United States v. White, 401 U.S. 745, 780 (1971) (Harlan, J., dissenting).

dislodge property principles from Fourth Amendment law. *Katz* was both consistent with and offered no clear alternative to the loose property approach. Absent a clear alternative to the traditional approach, a curious thing happened: very little changed. The Supreme Court considered a series of cases which required the Court to reaffirm or reject pre-*Katz* precedents in light of the new learning of *Katz*, and in case after case, the Court reaffirmed the earlier precedents. The *Katz* revolution proved a revolution more on paper than in practice. As a result, the Fourth Amendment today remains surprisingly similar to the Fourth Amendment before *Katz*.[126]

Consider just a few cases from the quarter-century that followed *Katz*. *United States v. White*[127] reaffirmed *On Lee v. United States*,[128] which had held that the police did not need a warrant to go undercover and wear a "wire" that transmitted the defendant's conversations to a police observation post. *Rakas v. Illinois*[129] reaffirmed *Gouled v. United States*,[130] which had held that Fourth Amendment rights are personal and cannot be asserted vicariously. *Oliver v. United States*[131] reaffirmed *Hester v. United States*,[132] retaining the quirky "open fields" doctrine. *California v. Hodari D.*[133] reaffirmed the common law rules governing when a person is "seized" under the Fourth Amendment.[134] These decisions are hard to square with a broad revolutionary reading of *Katz*.[135]

---

126. *See* John M. Junker, *The Structure of the Fourth Amendment: The Scope of the Protection*, 79 J. CRIM. L. & CRIMINOLOGY 1105, 1125 (1989) ("What is remarkable, however, is how little was changed by *Katz*. . . ."). *See also* David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739 (2000) (noting and criticizing the Supreme Court's reliance on common law standards in modern Fourth Amendment jurisprudence).

127. 401 U.S. 745, 750 (1971) ("We see no indication in *Katz* that the Court meant to disturb . . . the result reached in the *On Lee* case, nor are we now inclined to overturn this view of the Fourth Amendment.").

128. 343 U.S. 747 (1952).

129. 439 U.S. 128 (1978).

130. 255 U.S. 298 (1921).

131. 466 U.S. 170 (1984).

132. 265 U.S. 57 (1924).

133. 499 U.S. 621 (1991).

134. *Id.* at 624.

135. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 457 (1989) (Brennan, J., dissenting) ("[T]he plurality ignores the very essence of *Katz*."); California v. Ciraolo, 476 U.S. 207, 216 (1986) (Powell, J., dissenting) (arguing that the majority's property-based view "departs significantly from the standard developed in *Katz* for deciding when a Fourth Amendment violation has occurred"); Dow Chemical v. United States, 476 U.S. 227, 247 (1986) (Powell, J., concurring in part and dissenting in part) ("Today, while purporting to consider the Fourth Amendment question raised here under the rubric of *Katz*, the Court's analysis of the issue ignores the heart of the *Katz* standard."); Rakas v. Illinois, 439 U.S. 128, 162-63 (White, J., dissenting) ("Indeed, the decision today is contrary to Mr. Justice Brandeis' dissent in

Of course, it is debatable whether the continuing influence of property law remains normatively or doctrinally appropriate. The Supreme Court's opinions have sent conflicting rhetorical signals regarding the nature of the post-*Katz* Fourth Amendment. Sometimes the Court says that property is important to Fourth Amendment doctrine.[136] At other times, the Court has claimed that "the principal object of the Fourth Amendment is the protection of privacy rather than property,"[137] and has called *Katz* a "clear break"[138] from prior law.[139] In the period immediately following *Katz*, it made sense to

---

Olmstead v. United States, 277 U.S. 438, 478 (1928), expressing a view of the Fourth Amendment thought to have been vindicated by *Katz*.").

136. In *Rakas*, for example, the Court stated that "[o]ne of the main rights attaching to property is the right to exclude others. . .and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude." *Rakas*, 439 U.S. at 143 (citations omitted). The Court continued:

> Expectations of privacy protected by the Fourth Amendment, of course, need not be based on a common-law interest in real or personal property, or on the invasion of such an interest. These ideas were rejected both in *Jones*, *supra*, and *Katz*, *supra*. But by focusing on legitimate expectations of privacy in Fourth Amendment jurisprudence, the Court has not altogether abandoned use of property concepts in determining the presence or absence of the privacy interests protected by that Amendment.

Id.

The court also stated that expectations of privacy could be legitimate based on "understandings that are recognized and permitted by society." *Id.* However, the Court has effectively proven itself highly reluctant to recognize those "understandings," and instead relies heavily on real property law.

137. *See, e.g.*, Warden v. Hayden, 387 U.S. 294, 304 (1967).

138. Desist v. United States, 394 U.S. 244, 248 (1969) ("However clearly our holding in *Katz* may have been foreshadowed, it was a clear break with the past."). The *Desist* case held that *Katz* did not apply retroactively, which under the test in place that time allowed the Court to consider how different *Katz* was to prior law. The Court explained that Katz had finally held explicitly what later cases had signaled implicitly, that the strict trespass cases were no longer good law. *See id.* at 250 ("*Katz* for the first time explicitly overruled the 'physical penetration' and 'trespass' tests enunciated in earlier decisions of this Court.").

139. The Court also suggested (albeit less than coherently) that the reasonable expectation of privacy test has a normative component. In Smith v. Maryland, 442 U.S. 735, 740-41 n.5 (1979), Justice Blackmun wrote:

> Situations can be imagined, of course, in which *Katz*' two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation or [sic] privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.

Id.

This analysis is notably difficult to square with the Court's other Fourth Amendment cases. Justice Blackmun is plainly correct that a declaration that all homes will be subject to entry would not eliminate Fourth Amendment protection. However, the reason is not that

imagine that *Katz* might signal a dramatic shift.[140] But for better or worse, the Court has followed a more conservative path; conservative not so much in the political sense (although that may be true, as well), but in the sense that the Court's path generally has sought to preserve pre-*Katz* precedents. Most of the Court's majority decisions have in effect linked when an expectation of privacy was "reasonable" with whether it was backed by a loose version of the right to exclude, the traditional cornerstone of Fourth Amendment law.

Viewed in this light, much of the academic criticisms of the Court's post-*Katz* decisions fall a bit flat. To critics who insist that the "reasonable expectation of privacy" test is fundamentally normative, judicial decisions that deviate from the critic's normative views simply reflect unenlightened understandings of privacy, and are all wrongly decided.[141] Indeed, scholars consistently denounce the Court's

---

this would somehow trigger a "normative" inquiry, but because such a notice would not interfere with a homeowner's right to exclude. This is the same reason why Fourth Amendment protections in the home do not depend in any way on whether the defendant lives in a high crime neighborhood, has nosy neighbors, or keeps the front door unlocked. *See* United States v. Ross, 456 U.S. 798, 822 (1982) (noting that "the most frail cottage is absolutely entitled to the same guarantees of [Fourth Amendment] privacy as the most majestic mansion."). The Fourth Amendment protections derive from the right to exclude, and that does not depend on the mere likelihood that an invasion will occur.

140. Professor LaFave's treatise quotes extensively from legal scholarship from the late 1960s and early 1970s that views *Katz* as a radical break from existing law. *See* 1 LAFAVE, *supra* note 24, at 389-94. After quoting these sources, he laments that the Court has strayed: "Though this is the way that the second *Katz* prong *ought* to be interpreted, it is beyond question that the post-*Katz* decisions of the Supreme Court do not ordinarily or often square with the foregoing analysis." *Id.* at 394.

141. *See, e.g.*, LAFAVE, *supra* note 24, at § 2.7(c) at 631 ("The result . . . is dead wrong, and the Court's woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection which the Court developed in *Katz*."); Gerald G. Ashdown, *The Fourth Amendment and the 'Legitimate Expectation of Privacy'*, 34 VAND. L. REV. 1289, 1294 (1981) (explaining Supreme Court cases rejecting Fourth Amendment challenge brought under *Katz* to the Justices' "dissatisfaction with the exclusionary rule or a desire to accommodate state and local law enforcement," which has allowed the Court "to distort its perception of which privacy expectations are justifiable and deserving of protection."); Richard S. Julie, Note, *High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age*, 37 AM. CRIM. L. REV. 127, 131 (2000) ("Unfortunately, as members of the Warren Court retired and were replaced by more conservative members, the broad reading given [*Katz*] . . . began to be turned on its head."); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 554 (1990) ("The *Katz* standard has been twisted to allow the government access to many intimate details about our lives."); Jonathan Todd Laba, Comment, *If You Can't Stand the Heat, Get Out of the Drug Business: Thermal Imaging, Emerging Technologies, and the Fourth Amendment*, 84 CAL. L. REV. 1437, 1454 (1996) (arguing that although post-*Katz* cases claimed to be applying the *Katz* test, "this show of loyalty to *Katz* has proven specious, for subsequent cases have undermined the promise of *Katz*"); Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583, 587 (1989) (arguing that "the entire course of recent Supreme Court fourth amendment precedent, which has narrowed significantly the scope of individual activities that are protected constitutionally, is misguided and inconsistent with the spirit of the fourth amendment."); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings*

opinions interpreting *Katz* as "dead wrong,"[142] "off the mark,"[143] "misguided,"[144] and "inconsistent with the spirit of the fourth amendment."[145] To these scholars, *Katz* announced a true path that the Court subsequently failed to follow.[146] But a less revolutionary interpretation of *Katz* reveals a somewhat different picture. For better or worse, the Supreme Court has been fairly consistent in its approach to the Fourth Amendment: both before and after *Katz*, Fourth Amendment protections have mostly matched the contours of real property law.

C. *The Deference Norm in New Technologies*

The continuing influence of real property law on the modern Fourth Amendment has had a profound effect on how courts have applied the Fourth Amendment to new technologies. New technologies often destabilize the relationship between property and privacy.[147] Some technologies expose information that otherwise might have remained hidden; others conceal information that otherwise might have been exposed.[148] From the viewpoint of property law, these details are critical. In general, the police must interfere with property rights to discover what is hidden; "taking action . . . which expose[s] to view concealed [property]" is a Fourth Amendment search.[149] Because the police need not interfere with property rights to see that which is in plain view, the viewing of already exposed information generally is

---

Recognized and Permitted by Society", 42 DUKE L.J. 727, 732 (1993) (arguing that some Supreme Court cases "do not reflect societal understandings" of when an expectation of privacy is "reasonable," and that "some of the Court's conclusions [about what expectations of privacy are reasonable] may be well off the mark"); Tomkovicz, *supra* note 99, at 647 (explaining that post-Katz cases "neither fulfilled the promises of *Katz* nor been consonant with an appropriately conceived fourth amendment core.").

142. 1 LAFAVE, *supra* note 24, at 631.

143. Slobogin & Schumacher, *supra* note 141, at 732.

144. Serr, *supra* note 141, at 587.

145. *Id.*

146. For example, Professor LaFave's treatise quotes extensively from legal scholarship from the late 1960s and early 1970s suggesting that *Katz* will bring a radical break with existing law. *See* 1 LAFAVE, *supra* note 24, at 389-94. After quoting these sources, he then briefly notes that the Court has taken a very different path: "Though this is the way that the second *Katz* prong *ought* to be interpreted, it is beyond question that the post-*Katz* decisions of the Supreme Court do not ordinarily or often square with the foregoing analysis." *Id.* at 394.

147. *See* Kyllo v. United States, 533 U.S. 27, 33-34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

148. I develop this later in Part III.

149. Arizona v. Hicks, 480 U.S. 321, 325 (1987) (holding that moving stereo equipment to see the bottom of the equipment is a search).

not a search under the Fourth Amendment.[150] When new technologies change what is exposed and what is hidden, the scope of Fourth Amendment protections can shift depending on the details of how the technologies work.

This dynamic has often led to a relatively modest and deferential Fourth Amendment in the area of developing technologies. Granted, when technology leads to the hiding of information that in the past would have been exposed, technological advance can expand Fourth Amendment protection. Consider the use of tinted windows on automobiles. Under the property-based Fourth Amendment, the police can look inside a car through a clear window.[151] Looking through the window is not a search.[152] Tinted windows, however, can block the ability of the police to see what is inside. To look behind a tinted window, the police might need to open the door or break the window, both of which interfere with property rights and qualify as Fourth Amendment searches. At least where not prohibited by substantive law, tinted windows can expand privacy by hiding what was once exposed; by expanding what property protects, the new technology expands the scope of Fourth Amendment protection.

This dynamic is relatively rare, however. New technologies more commonly expose information that in the past would have remained hidden, resulting in meager Fourth Amendment protection in new technologies. Examples are plentiful. In *California v. Ciraolo*,[153] the Supreme Court considered the Fourth Amendment implications of aerial surveillance enabled by the invention of the airplane. Investigators flew an airplane above the defendant's backyard, and from public airspace looked down to see whether the defendant was growing marijuana in the yard.[154] The yard was surrounded by double fences, but the airplane allowed the police to observe the marijuana without interfering with them. The Court upheld the surveillance, ruling that because the plane was flown "within public navigable airspace. . .[and] in a physically nonintrusive manner"[155] — that is, without violating the defendant's property rights — the practice did not violate the defendant's reasonable expectation of privacy.[156]

The Court took the same approach when it considered the Fourth Amendment implications of chemical tests that can detect the

150. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). *Cf.* Colb, *supra* note 87, at 124-26 (discussing the "exposure" line of Fourth Amendment cases).

151. Texas v. Brown, 460 U.S. 730, 739-40 (1982).

152. *Id.*

153. 476 U.S. 207 (1986).

154. *Id.* at 209.

155. *Id.* at 213 (citation omitted).

156. *See id.* at 213-14.

presence of illegal narcotics. In *United States v. Jacobsen*,[157] the Court reasoned that such tests do not violate a defendant's reasonable expectation of privacy because cocaine ownership is illegal.[158] Because contraband cocaine cannot be legally owned, a defendant cannot claim a "legitimate" right in cocaine, and a chemical test that is limited in scope to determining the presence of illegal narcotics cannot violate a reasonable expectation of privacy.[159]

Courts have taken a similar approach with records generated by communications technologies such as the telephone and the Internet. As several commentators have noted, communications technologies allow owners and operators of communications networks to build complete dossiers on their users.[160] The telephone company can know exactly when a particular telephone line was used to place a particular call, the number dialed, and the length of the call. Internet service providers ("ISPs") can keep records of session times, websites visited, and e-mails sent and received.[161] This information can allow providers to assemble a comprehensive picture of their users' private conduct. Courts have held that the Fourth Amendment protects little, if any, of this information. Under the property-based approach,

> the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[162]

Once a user discloses information to the provider, the user relinquishes any Fourth Amendment protection in the information by virtue of losing the right to exclude. Although the information may

---

157. 466 U.S. 109 (1984).

158. *See Jacobsen*, 466 U.S. at 123; *see also* Warden v. Hayden, 387 U.S. 294, 302 (1967) (defining contraband as an item for which "a valid exercise of the police power renders possession of the property by the accused unlawful and provides that it may be taken" (quoting Gouled v. United States, 255 U.S. 298, 309 (1921))). Common examples of items that fall within this definition include child pornography, United States v. Kimbrough, 69 F.3d 723, 731 (5th Cir. 1995), pirated software and other copyrighted materials, United States v. Vastola, 670 F. Supp. 1244, 1273 (D.N.J. 1987), counterfeit money, narcotics, and illegal weapons.

159. *Jacobsen*, 466 U.S. at 123.

160. *See id.* at 123; *see also* Solove, *supra* note 7, at 1084 ("In the Information Age, an increasing amount of personal information is contained in records maintained by Internet Service Providers (ISPs), phone companies, cable companies, merchants, bookstores, websites, hotels, landlords, employers and private sector entities.").

161. *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 612-15 (2003) [hereinafter Kerr, *Internet Surveillance*]. (explaining the different records that Internet service providers can maintain relating to their users).

162. United States v. Miller, 425 U.S. 435, 443 (1976).

still seem private, the government does not violate any principle of property law by asking a third-party to disclose it.

Following this principle, the Supreme Court held in *Smith v. Maryland*[163] that telephone users do not have a "reasonable expectation of privacy" in the telephone numbers that they dial because the numbers disclosed to the telephone company.[164] Courts have applied the same principle to information disclosed to Internet service providers[165] and Western Union.[166] Lower courts have also applied this approach to the interception of cordless telephone calls. Although the Supreme Court has never ruled on this question, lower courts have held that government interception of a cordless phone call does not violate the Fourth Amendment.[167] Why? Unlike traditional landline telephones, cordless phones broadcast a signal that can be picked up by others. Although intercepting a cordless phone call invades privacy, it invades privacy without invading property: the intercepting device merely picks up a signal that has been "broadcast over the radio waves to all who wish to overhear,"[168] and is therefore available to the public.[169] The courts have adopted similar rationales to reject claims of Fourth Amendment protection for other types of radio transmissions.[170]

---

163. 442 U.S. 735, (1979).

164. Id. at 742.

165. *See* Guest v. Leis, 225 F.3d 325, 335-36 (6th Cir. 2001) (finding no expectation of privacy in non-content information disclosed to ISP); United States v. Hambrick, 55 F. Supp. 2d 504, 508-09 (W.D.Va. 1999), *aff'd* 225 F.3d 656, 2000 WL 1062039 (4th Cir. 2000) (unpublished table decision) (same); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D.Kan. 2000) (same).

166. *See In Re* Grand Jury Proceedings, 827 F.2d 301, 302-03 (8th Cir. 1987) (holding that Western Union customers have no reasonable expectation of privacy in Western Union records concerning the customers' activities).

167. *See, e.g.*, Price v. Turner, 260 F.3d 1144, 1149 (9th Cir. 2001); United States v. McNulty (*In re* Askin), 47 F.3d 100, 104-106 (4th Cir. 1995) (involving a call made to a cordless telephone user); McKamey v. Roach, 55 F.3d 1236, 1239-40 (6th Cir. 1995); Tyler v. Berodt, 877 F.2d 705, 707 (8th Cir. 1989) (involving a call from a cordless phone). Notably, however, at least one court has suggested that as the technology becomes more advanced and such phone calls are harder to intercept, interception may begin to violate the Fourth Amendment because it would be more "reasonable" to expect privacy against interception. *See, e.g.*, United States v. Smith, 978 F.2d 171, 180 (5th Cir. 1992) ("Although we express no opinion as to what features or circumstances would be necessary to give rise to a reasonable expectation of privacy, it should be obvious that as technological advances make cordless communications more private at some point such communication will be entitled to Fourth Amendment protection.").

168. *McKamey*, 55 F.3d at 1239-40.

169. Of course, Congress can protect such calls when the Fourth Amendment does not. In the case of cordless telephone calls, Congress added statutory protection against their interception in 1994. *See id.* at 1238 n.1.

170. *See, e.g.*, United States v. Rose, 669 F.2d 23, 25 (1st Cir. 1982) (rejecting a claim of Fourth Amendment protection in an intercepted radio transmission); United States v. Peterson, 812 F.2d 486 (9th Cir. 1987).

These cases suggest that courts generally do not engage in creative normative inquiries into privacy and technological change when applying the Fourth Amendment to new technologies. For better or for worse, courts have tended to apply the same property-based principles to such cases that they have applied elsewhere. This has focused attention on whether government investigators collect information that technology has hidden or information that technology has exposed. Because many technologies expose new forms of information rather than hide them, the property law principles driving the Fourth Amendment have led to only weak Fourth Amendment protections in new technologies.[171]

D. *Property-Defeating Surveillance Technologies:* Knotts, Karo, *and* Kyllo

The Court's broad commitment to property principles in Fourth Amendment law has been tested by cases involving property-defeating surveillance technologies, and in particular *United States v. Knotts*,[172]

---

171. A student note in the *Yale Law Journal* from 1996 has led some commentators to reach a similar conclusion, albeit for an incorrect reason. *See* Adler, *supra* note 7. In this Note, the author concludes that the Fourth Amendment balancing test for reasonableness will gut Fourth Amendment protections involving computers because the government may be able to create new search tools that can conduct "perfect" searches. Specifically, the author argues that the reasonableness of a Fourth Amendment search depends on how narrowly tailored the search is, and reasons that Internet technologies will allow the government to execute searches online without warrants because Internet search tools can be used in very narrowly tailored ways. *See id.* at 1106.

Although this framework has been accepted by several commentators, *see, e.g.*, LESSIG, *supra* note 10, at 17-19, ROSEN, *supra* note 21, at 38-40, I believe that it is incorrect from the standpoint of existing Fourth Amendment doctrine. Adler fails to recognize that the Supreme Court's Fourth Amendment balancing cases generally deal with searches conducted for non-law-enforcement reasons. In these so-called "special needs" cases, the government is allowed a more relaxed standard so long as the non-law-enforcement need outweighs the privacy intrusion. For example, *Camara v. Municipal Court*, 387 U.S. U.S. 523 (1967), held that government housing inspectors could enter homes in a limited capacity to inspect homes for housing code violations. And in *Terry v. Ohio*, 392 U.S. 1 (1968), the Court held that a cop could briefly frisk a suspect for weapons to protect the officer's safety.

Adler's framework improperly assumes that this relaxed balancing test would also apply to government searches executed for traditional law enforcement purposes. The courts have not allowed this, however. When a search is conducted for a law enforcement purpose, courts do not apply a balancing test or weigh the intrusiveness of the search. Rather, the search itself violates a reasonable expectation of privacy, requiring either a warrant or an exception to the warrant requirement such as exigent circumstances, no matter how narrowly tailored or unobtrusive the search may be. *See, e.g.*, Nat'l Federation of Fed. Empl. v. Weinberger, 818 F.2d 935, 943 n.12 (D.C. Cir. 1987) ("The government may not take advantage of any arguably relaxed . . . standard for warrantless searches . . . when its true purpose is to obtain evidence of criminal activity. . . ."). Note that the Fourth Amendment generally does not allow police officers who are particularly skilled at finding evidence of crime to execute more warrantless searches than those who are not. This is true because whether the officer can execute a narrowly tailored search is normally not relevant to the Fourth Amendment inquiry. The same goes for searches undertaken remotely by computers, or through any other technological means.

172. 460 U.S. 276 (1983).

United States v. Karo,[173] and *Kyllo v. United States*.[174] In these cases, police used new surveillance technologies that threatened to eliminate property as a guide to what is hidden and what is exposed in the home. Here the Court has deviated from a strict focus on how the technology works and instead created rules to preserve the degree of surveillance authority in the home that property law principles have traditionally allowed. Although these cases (and particularly *Kyllo*) can be read plausibly as suggesting a broad and even creative view of how the Fourth Amendment should respond when technology threatens privacy, I think a better reading is that these cases are essentially conservative, reinforcing the primacy of property law. The cases carve out an exception to the usual methodology to achieve the traditional goal of property protection in the home, but at least so far do not signal a broader commitment to expansive Fourth Amendment protections in new technologies.

The first of these cases is *United States v. Knotts*,[175] which involved the use of an electronic tracking device to investigate a methamphetamine manufacturing ring. To monitor the conspiracy, the police placed a radio transmitter that emitted periodic signals inside a five gallon drum of chemicals used to manufacture methamphetamine. The drum was then sold to a member of the conspiracy named Petschen, who kept the drum (and with it, the tracking device) in his car.[176] The police traced Petschen's location based on the signals they received from the transmitter, and learned that Petschen had driven the car on to Knotts's property. The police used this information to obtain a warrant to search Knotts' farm, where they discovered "a fully operable, clandestine drug laboratory."[177] Knotts then challenged the warrantless use of the tracking device (but not its installation, oddly enough) as a violation of the Fourth Amendment.

The Court concluded that the warrantless use of the tracking device did not violate the Fourth Amendment because the information that the police obtained using the surveillance technology was essentially public. The police *could* have obtained the same information by "following Petschen at a distance throughout his journey,"[178] which would not have required a warrant. In other words, what really mattered was not the technical details of *how* the information was obtained — the usual inquiry — but rather *what* information was obtained. Because the location of Petschen's car was

173. 468 U.S. 705 (1984).

174. 533 U.S. 27 (2001).

175. 460 U.S. 276 (1983).

176. *See id.* at 279.

177. *Id.*

178. *Id.* at 285.

the kind of public information that any onlooker could observe, it did not violate the Fourth Amendment to invade Petschen's property rights to obtain it.

The flip side of *Knotts* arrived the next year in *United States v. Karo*.[179] The facts of *Karo* closely resemble those of *Knotts*: an electronic tracking device was placed in a container and sold to a suspected co-conspirator in a narcotics ring.[180] The police then learned the whereabouts of the conspiracy by following the tracking device. In *Karo*, however, the defendant brought the container into several private homes, and the signal allowed the police to know that the container was inside those homes.[181] Once again the police used the information to obtain a warrant, and a search of the homes revealed a narcotics operation. This time, however, the Court ruled that the surveillance violated the defendant's reasonable expectation of privacy.[182] Why the difference? Because this time the tracking device had sent a signal from "a private residence, a location not open to visual surveillance."[183] The information obtained through the tracking device was information that a police officer normally would need to enter the home to obtain,[184] and since entering a home was a search, so was using a tracking device inside one.[185] Once again, the Court looked to whether the police traditionally would have needed a warrant to collect the information that they collected.

This brings us to *Kyllo v. United States*,[186] the Court's recent decision on thermal imaging devices. *Kyllo* involved a camera that

---

179. 468 U.S. 705 (1984).

180. *Id.* at 707.

181. *Id.* at 709-10.

182. *Id.* at 717.

183. *Id.* at 714.

184. The Court observed:

> In this case, had a DEA agent thought it useful to enter the . . . residence to verify that the ether was actually in the house and had he done so surreptitiously and without a warrant, there is little doubt that he would have engaged in an unreasonable search within the meaning of the Fourth Amendment.

Id. at 715.

185. According to the Court, a contrary rule "would present far too serious a threat to privacy interests in the home. . ." *Id.* at 716. In a partial concurrence, Justice Stevens noted that this result matched the Court's usual property-based approach to the Fourth Amendment as well, but the majority focused solely on assessing the privacy implications of the information:

> When the Government attaches an electronic monitoring device to [a defendant's] property, it infringes that exclusionary right; in a fundamental sense it has converted the property to its own use. Surely such an inversion is an "interference" with possessory rights; the right to exclude, which attached as soon as the can respondents purchased was delivered, had been infringed.

Id. at 729 (Stevens, J., concurring in part and dissenting in part).

186. 533 U.S. 27 (2001).

detected infrared radiation, a type of radiation that all objects emit naturally.[187] The human eye does not normally detect this radiation because the wavelength of the light is longer than visible light. Certain chemicals can detect and measure this radiation, however, which allows "infrared cameras" to be designed that can take a picture of the infrared light emitted by the object viewed.[188] Such cameras are often known as "thermal imaging devices" because the amount of infrared light an object emits varies based on the object's temperature.[189] By measuring the infrared radiation emitted by an object, the thermal imaging device determines the temperature of the surface of the object, down to a depth of about one-thousandth of an inch.[190]

In *Kyllo*, the police directed an infrared thermal imaging device at the exterior of the defendant's home to help establish that the defendant was growing marijuana inside his home.[191] The device reported that the roof over the garage and a side wall of the Kyllo's home were unusually hot, likely evidence of heat lamps being used to help grow marijuana inside.[192] The police used the thermal image to create a case for probable cause to justify a search of the home, and the resulting search warrant led to the discovery that Kyllo was in fact growing marijuana under lights.[193] Kyllo argued that the use of the infrared device violated his Fourth Amendment rights, but the Ninth Circuit rejected the claim.[194] The Ninth Circuit agreed with the unanimous judgment of others Courts of Appeals that imaging did not violate a reasonable expectation of privacy because the imaging device merely received and recorded the infrared radiation, much like the human eye merely received radiation in the form of visible light.[195] These decisions focused on how the technology worked: because the imaging device merely observed passively, it did not actively "search" the home.

The Supreme Court reversed.[196] Writing for a 5-4 majority, Justice Scalia followed *Karo* and *Knotts*: the use of the imaging device was a Fourth Amendment 'search,' Scalia wrote, because it used technology to obtain "information regarding the interior of the home that could

187. *Id.* at 31.

188. *See* J. M. LLOYD, THERMAL IMAGING SYSTEMS 2 (1997).

189. *See id.*

190. *See id.* at 2-5.

191. *Kyllo*, 533 U.S. at 29.

192. *Id.*

193. *Id.*

194. United States v. Kyllo, 190 F.3d 1041 (9th Cir. 1999).

195. *See id.* at 1045.

196. Kyllo v. United States, 533 U.S. 27 (2001).

not otherwise have been obtained without physical intrusion."[197] Granted, the device did not actually 'see' inside the home, but the information obtained by measuring the temperature of the *outside* of the home provided a great deal of information about the likely temperature *inside* the home, information the Court construed as private.[198] The Court concluded that "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[199] This test is rather mystifying from the standpoint of physics,[200] but matches the general approach of *Knotts* and *Karo*. Just as *Knotts* and *Karo* measure the intrusiveness of tracking devices compared to the bench mark of visual surveillance, *Kyllo* measures the intrusiveness of sense-enhancing devices directed at the home compared to the traditional benchmark of physical intrusion.

At first blush, *Kyllo* and *Karo* may appear to embrace expansive Fourth Amendment protections in new technologies. I think it is more accurate to understand these cases as conservative decisions. They are conservative in that they are trying to retain the very core of traditional Fourth Amendment protections: the protection of information about the home traditionally enforced by property law. Tracking devices and thermal imaging devices threaten to expose information within the home that property has traditionally hidden; they reveal the location and temperature of items inside the home not visible with the naked eye. Faced with technologies that threaten to defeat property's ability to safeguard traditional privacy protections in the home, the Court has fashioned new rules in an effort to retain the traditional protections set by property law. These cases differ from the rest of the Court's property-based decisions in that they do not focus on how the technology works or on whether information obtained has been exposed or hidden. But they do so in a narrow way to achieve the traditional goal of Fourth Amendment protection in the home.

Lower court interpretations of *Karo* and *Kyllo* reinforce the modesty of this enterprise. Both cases have been interpreted quite narrowly. For example, the lower courts have not expanded *Karo*

197. *Id.* at 534 (internal quotations omitted).

198. *See id.* at 40 (Stevens, J., dissenting).

199. *Id.*

200. The difficulty is that under *Kyllo* the frequency of light determines whether it receives Fourth Amendment protection. Light in the visible spectrum does not receive Fourth Amendment protection: looking at an object using human eyes is not search. However, light in the infrared spectrum is protected by the Fourth Amendment, at least when the object emitting the infrared light is a home. From the standpoint of physics, this is something like saying that the government needs a search warrant to look at blue objects but not red objects.

beyond the specific domain of tracking devices. *Karo* is cited most frequently for the principle that the Fourth Amendment offers special protections to the home.[201] Most of the other cases citing *Karo* deal with specific factual variations involving tracking devices, and particularly the line between *Karo* and *Knotts*. For example, the Fourth Circuit has held that locating a stolen mail bag that contains a tracking device is closer to *Knotts* than *Karo*.[202] One district court concluded that using tracking device placed in postal mail is closer to *Karo* than *Knotts*;[203] and another district court held that placing a tracking device on a sailing ship is closer to *Knotts* than *Karo*.[204] One federal district court relied on *Karo* to reject a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) when the plaintiff in a *Bivens* action made a general claim that the defendants had "surveilled" him,[205] but the unpublished opinion doesn't explain whether the result had anything to do with the specific holding of *Karo*.[206] Beyond that, the courts have not found *Karo* and *Knotts* relevant to broader questions in Fourth Amendment law, and when *Karo* has been raised by defendants, courts have declined to extend its approach to other areas.[207]

Kyllo has met a similar fate, at least so far. It has been cited mostly for the same proposition as *Karo*: that the Fourth Amendment offers special protections to the home.[208] *Kyllo* has been applied to other cases involving the use of a thermal imaging device directed at a

---

201. *See, e.g.*, United States v. James Daniel Good Real Property, 510 U.S. 43, 53-54 (1993) ("Good's right to maintain control over his home, and to be free from governmental interference, is a private interest of historic and continuing importance." (citing United States v. Karo, 468 U.S. 705, 714-715 (1984))).

202. United States v. Jones, 31 F.3d 1304 (4th Cir. 1994).

203. United States v. Dowdy, 688 F. Supp. 1477 (D. Colo. 1988).

204. United States v. Juda, 797 F. Supp. 774, 783 (N.D. Cal. 1992).

205. Altieri v. Pennsylvania State Police, No. Civ.A.98-CV-5495, 2000 WL 427272 (E.D. Pa. Apr. 19, 2000) (unpublished opinion).

206. *See id.* at *3.

207. For example, in United States v. Colyer, 878 F.2d 469 (D.C. Cir. 1989), the D.C. Circuit rejected the argument that *Karo* and *Knotts* were relevant to the question of whether a dog sniff that led to the discovery of narcotics was a Fourth Amendment search. The court found *Knotts* and *Karo* "factually distinct" and of only "marginal" relevance. *See id.* at 474 n.5

Notably, however, a handful of lower court decisions relied on *Karo* to conclude that thermal imaging devices violate the Fourth Amendment, an approach the Supreme Court adopted in *Kyllo*. *See* United States v. Elkins, 95 F. Supp. 2d 796, 812 (W.D. Tenn. 2000), *modified*, 300 F.3d 638 (6th Cir. 2002); United States v. Cusumano, 67 F.3d 1497, 1507 (10th Cir. 1995), *vacated*, 83 F.3d 1247, 1250-51 (10th Cir. 1996) (en banc) (declining to "decide the constitutionality of the warrantless use of the thermal imager. . ."); United States v. Field, 855 F. Supp. 1518, 1530 (W.D. Wisc. 1994).

208. Loria v. Gorman, 306 F.3d 1271 (9th Cir. 2002); United States v. Tolar, 268 F.3d 530, 532 (7th Cir. 2001).

home.[209] But no judicial opinion has extended the holding of *Kyllo* to any other fact pattern to broaden the scope of Fourth Amendment protections. One Sixth Circuit decision ponders but does not decide whether *Kyllo* applies to use of a thermal imaging device directed at a commercial building.[210] One unpublished district court decision[211] contemplates but does not decide whether *Kyllo* implicitly overruled *United States v. Place*,[212] which had held that a dog sniff of a package (for drugs) was not a "search."[213] But no case has taken *Kyllo* beyond the facts of the case itself, and no court has viewed *Kyllo* as a symbolic endorsement of broad privacy rights in new technologies. Ironically, the one post-*Kyllo* case relying on the decision in substance (albeit questionably) used *Kyllo* to *narrow* the scope of Fourth Amendment protection, rather than broaden it.[214] While *Kyllo* has been hailed as a "landmark"[215] in the law reviews, so far it has hardly made a peep in the courts.

---

209. As the Ninth Circuit recently noted:

> Depew's argument that law enforcement agents entered the curtilage of his house when they conducted a thermal scan of the building has been rendered moot by the Supreme Court's recent decision in *Kyllo v. United States*, 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). Under *Kyllo*, the thermal scan was a search, and hence violated the Fourth Amendment, no matter where the agents were standing when they conducted it. The information gained from the thermal scan therefore cannot be used to support the probable cause determination underlying the search warrant that was issued.

United States v. Depew, 17 Fed. Appx. 563, 563-64 (9th Cir. 2001).

210. United States v. Elkins, 300 F.3d 638, 647 (6th Cir. 2002).

211. United States v. Richard, No. CRIM. 01-20048-01, 2001 WL 1033421, at *6 n.4 (W.D. La. Aug. 29, 2001).

212. 462 U.S. 696 (1983).

213. *See id.* at 707.

214. In *United States v. Maple*, 334 F.3d 15 (D.C. Cir. 2003), a police officer looked inside the front console of an automobile between the two front seats to find a place to put the defendant's cellular phone. When he opened the console, he found an illegal pistol. Judge Silberman held that the opening of the console was constitutional, relying at least in part on *Kyllo*. *See id.* at 19-20. *Kyllo* had introduced an originalist interpretation of "search," which according to Justice Scalia meant to look through "for the purpose of finding something." *Id.* at 19 (citing *Kyllo*, 533 U.S. 27, 33 n.1 (2001)). Judge Silberman reasoned that under *Kyllo*, no search had occurred, because the officer had not been looking for anything when he opened the console. *See id.* at 20. This is notably incorrect from the standpoint of the property-based approach to the Fourth Amendment; by opening the defendant's console, the police officer interfered with the defendant's right to exclude others from the console, triggering the Fourth Amendment. *See id.* at 24 (Rogers, J., dissenting) ("Under the Supreme Court's precedents, . . . the officer's opening of the closed compartment . . . constituted a search . . . .").

215. *See, e.g.*, Cole, *supra* note 6, at 7. *See also* Sklansky, *supra* note 7, at 144-45 (describing *Kyllo* as a "likely touchstone[]" for future Supreme Court cases on the Fourth Amendment, concluding that its reasoning was "expansive," and that the case has "significance beyond its narrow holding and beyond its value as a curiosity"). *Cf.* Arbus, *supra* note 7, at 1769 (arguing that *Kyllo* helped begin "a new era of Fourth Amendment jurisprudence").

E. *Why the Fourth Amendment Alone Cannot Protect Privacy in New Technologies*

This Article has so far challenged the doctrinal foundations of what I have labeled the popular view of the Fourth Amendment in new technologies. It has made a descriptive doctrinal claim: while *Katz* had revolutionary promise, cases interpreting *Katz* and the "reasonable expectation of privacy" test have mostly focused on the details of how new technologies work and whether they interfere with traditional property rights. Most existing Fourth Amendment rules in new technologies are based heavily on property law concepts, and as a result offer only relatively modest privacy protection in new technologies. The cases are not entirely consistent. But understood as a whole, the existing body of doctrine reflects a relatively humble and deferential judicial attitude.

The key implication of this deferential stance is that we should not expect the Fourth Amendment alone to provide adequate protections against invasions of privacy made possible by law enforcement use of new technologies. The popular view effectively equates a reasonable expectation of privacy with the expectation of privacy that a reasonable person would expect. If this were the case, legislative privacy protections would be unnecessary. After all, the normative expectations of privacy of a reasonable person are the same as the governing privacy rules that a reasonable person would want, which are the same as the rules that an idealized legislature would enact. If the Fourth Amendment set such goals and courts could achieve them competently, there would be no need for legislative action. Existing precedents suggest a different practice, however. A "reasonable expectation of privacy" has not been equated with the expectation of privacy of a reasonable person; rather, it has been used as a term of art based heavily on property law principles. As a result, existing Fourth Amendment rules are not necessarily the rules that sensible legislators might enact and reasonable citizens might desire. Especially in the area of high technology, the property-based Fourth Amendment does not guarantee that the rules governing law enforcement are optimal rules that effectively balance the competing concerns of privacy and effective law enforcement.

Additional privacy protections are needed to fill the gap between the protections that a reasonable person might want and what the Fourth Amendment actually provides. As we will see in the next part, those protections historically have come from Congress. And as we will see in the final Part, Congress will likely remain the primary source of privacy protections in new technologies thanks to institutional advantages of legislatures.

II. WIRETAPPING LAW AND LEGISLATIVE REGULATION OF GOVERNMENT INVESTIGATIONS INVOLVING NEW TECHNOLOGIES

The popular view that the Fourth Amendment should be interpreted broadly in cases involving new technologies often relies explicitly or implicitly on the history of the Fourth Amendment. Proponents sometimes tell a story that goes something like this: in the beginning, the *Olmstead* majority failed to recognize that the Fourth Amendment should regulate wiretapping. *Olmstead* prevailed for forty years, during which wiretapping and other invasive government surveillance practices remained rampant.[216] Everything changed when the Supreme Court decided *Katz v. United States* in 1967. The *Katz* majority adopted Justice Brandeis's *Olmstead* dissent and constitutionalized wiretapping law,[217] ushering in a constitutional order.[218] The moral of the story is that courts can step in and successfully constitutionalize law enforcement practices involving new technologies. Although wiretapping law is only one corner of high-tech privacy law, the wiretapping example offers an optimistic lesson: just as the Supreme Court saved wiretapping law decades ago, so can future courts step in and create protective Fourth Amendment rules regulating law enforcement use of new technologies effectively. If in doubt, just look at the transition from *Olmstead* to *Katz*.

This Part explores the history of wiretapping law and concludes that this account overstates the impact of the Fourth Amendment and understates the role of legislative privacy protections. To be sure, *Katz* and *Berger* remain good law, and modern wiretapping law reflects their influence. But from its inception in the mid-nineteenth century through the present, wiretapping law has remained a primarily statutory field governed by statutory commands. Indeed, it turns out that very few cases in the history of wiretapping law have ruled that a wiretapping practice violated the Fourth Amendment. Despite the big splash of *Berger* and *Katz*, later courts generally have declined to

---

216. As Professor Gormley writes:

> By the 1950s, the technology that enabled government surveillance had grown by exponential leaps. Parabolic microphones, transmitters the size of cigarette packs, induction-coil devices and miniature television transmitters made it possible for government agents, police, private investigators and average citizen snoopers to watch, listen and record virtually any sound or movement. Accompanying this perfection in technology came the growing use of private detectives as surreptitious information-gatherers in business and family disputes, extending the intrusive scope of eavesdropping to the private sector. Attempts by the states to curb or prohibit wiretapping were largely ineffective.... By the time the United States entered the 1960s, most of the attempts to protect individual privacy by curbing electronic surveillance at the state level had failed.

Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1363 (1992).

217. *See supra* note 86.

218. *See, e.g.*, Lessig, *supra* note 10, at 116-18; Ric Simmons, *Can Winston Save Us from Big Brother? The Need for Judicial Consistency in Regulating Hyper-Intrusive Searches*, 55 RUTGERS L. REV. 547, 562-64 (2003).

extend privacy against wiretapping beyond statutory commands. Fourth Amendment decisions have affected the shape of legislation in important ways, but legislation rather than the Fourth Amendment has provided the primary protection against invasions of privacy from wiretapping. To some extent, this is not exactly news: pick up any practitioner's treatise on wiretapping law and you will find that it is concerned primarily with statutory law.[219] At the same time, the extent to which courts have refused to regulate wiretapping practices via judicial standards post-*Katz* is quite surprising. Wiretapping law is more legislative and less constitutional than many realize.

This Part examines the history of wiretapping law, with a focus on the source of legal protections. I divide the history of wiretapping law into four periods: first, pre-1934, including the period before and during the National Prohibition Act;[220] second, from 1934 until 1967; third, from 1967 to 1968, involving the critical period of *Berger v. New York*,[221] *Katz v. United States*,[222] and the enactment of the federal Wiretap Act; and fourth, the modern era following the passage of the Wiretap Act. I argue that within each period, statutory protections rather than constitutional limits have been the primary regulators of wiretapping law and practice. I conclude by suggesting that the statutory regulation of wiretapping may be more the rule than the exception. While commentators have focused their attention on constitutional decisions, Congress has passed dozens of statutory laws that regulate law enforcement practices implicating new technologies. If wiretapping law provides a case study of whether courts or legislatures take the lead role in regulating privacy in new technologies, that case study suggests that Congress plays the lead, not the courts.

A. *The Origins of Wiretapping Law: Prohibition, Early Statutory Protections, and the* Olmstead *Case*

Wiretapping is the use of a device to intercept an electric or electronic communication sent over a wire. The practice of wiretapping by private parties became common soon after the arrival

219. *See, e.g.*, James G. Carr, Electronic Surveillance; Clifford S. Fishman & Anne T. McKenna, WIRETAPPING AND EAVESDROPPING (2d ed. 1995).

220. Act of Oct. 28, 1919, ch. 85, 41 Stat. 305 (repealed 1933).The National Prohibition Act was widely known as the Volstead Act, after Andrew J. Volstead, the Minnesota Congressman who introduced it in the House of Representatives. *See generally* Sidney J. Spaeth, *The Twenty-First Amendment And State Control Over Intoxicating Liquor: Accommodating The Federal Interest*, 79 CAL. L. REV. 161, 176 (1991).

221. 388 U.S. 41 (1967).

222. 389 U.S. 347 (1967).

of the telegraph (invented by Samuel Morse in 1837[223]) and telephone (invented by Alexander Graham Bell in 1876). Business competitors and private snoops tapped lines, listening in on private conversations and often using that information for private gain.[224] Legislatures and the public recognized the invasiveness of wiretapping quite early. California passed a statute that prohibited tapping telegraph lines in 1862.[225] Telephone wiretapping was prohibited in New York and Illinois in 1895; California extended its ban on telegraph interception to telephones in 1905.[226] Other states followed: by 1928, more than half of the states had enacted criminal bans on wiretapping.[227] The federal government also enacted a criminal ban on wiretapping in early 1918 for the remainder of World War I, a period when the federal government took over control of both telephone and telegraph lines.[228] Prosecutions for illegal wiretapping remained rare, however.[229]

No published decisions prior to the National Prohibition Act in 1919 considered whether wiretapping violated the Fourth Amendment.[230] This may surprise modern ears at first, but the context of early federal law enforcement helps explain it. Before Prohibition, the scope of the Fourth Amendment was rarely litigated. The Fourth Amendment regulated only the Federal government, not the states,[231] and the Federal government brought only a few thousand criminal

---

223. *See* EDWARD V. LONG, THE INTRUDERS 36 (1967).

224. *See id.* at 30-35.

225. Berger v. New York, 388 U.S. 41, 45 (1967) (citing Statutes of California, 1862, p.288, CCLX II).

226. *See id.*

227. *See id.*

228. *See* Law of Oct. 29, 1918, ch. 197, 40 Stat. 1017. *See generally Wiretapping, Congress, and the Department of Justice*, 9 INT'L JURID. ASS'N MONTHLY BULL. 97 (1941).

229. *See* Margaret Lybolt Rosenzweig, *The Law of Wire Tapping*, 32 CORNELL L. Q. 514, 514 (1947) ("Prosecutions [in the early days] seem to have been rare."). For an example of such a prosecution, see *State v. Behringer*, 172 P. 660 (Ariz. 1918). Wiretapping practices by state and local police varied considerably. SAMUEL DASH, ET. AL., THE EAVESDROPPERS (1959). Although the record remains sparse, it appears that some state police agencies wiretapped defendants, but others did not. When the police did wiretap defendants the evidence was generally admitted in court even in states where the wiretapping was itself illegal and the officer could be (and on rare occasion was) prosecuted. *See, e.g.*, People v. Hebberd, 35 N.Y. Crim. R. 165 (1916) (prosecuting a police officer for wiretapping in the course of his official duties). While this may seem remarkable today, it reflected the prevailing common law rule that the defendant could not challenge evidence on the basis of how it was collected. *See* State v. McDonald, 177 A.D. 806, 810 (N.Y. 1917) ("The only question before the trial court is the relevancy and materiality as evidence of such papers, documents, or conversations, and no collateral inquiry as to whether they were legally or illegally secured will be permitted to interrupt and disorganize the trial."); Rosenzweig, *supra*, at 515 ("The general rule that the illegal manner in which evidence was obtained is not a valid objection to its admissibility has its roots far back in the common law.").

230. Act of Oct. 28, 1919, ch. 85, 41 Stat. 305 (repealed 1933).

231. This conclusion was overruled in form in *Wolf v. Colorado*, 338 U.S. 25 (1949) and in substance in *Mapp v. Ohio*, 367 U.S. 643 (1961).

cases nationwide per year.[232] In addition, Congress did not routinely permit defendants to appeal their federal convictions until 1889.[233] As a result, the Supreme Court mentioned the Fourth Amendment in only about two dozen cases in the first 130 years of the Amendment's existence, and actually interpreted the Amendment only a handful of times in that period.[234] None of those cases involved wiretapping. Indeed, no published federal criminal cases mentioned wiretapping before the Prohibition era.[235]

The National Prohibition Act of 1919 changed everything.[236] The number of federal criminal cases skyrocketed,[237] and the national prohibition on the transportation or distribution of alcohol created the need for an infrastructure that could support large-scale federal law enforcement.[238] The number of search warrants obtained by federal officers spiked dramatically, as agents obtained warrants to search for and seize the contraband of illegal alcohol.[239] The federal courts began

---

232. *See* Michael A. Simons, *Prosecutorial Discretion and Prosecution Guidelines: A Case Study in Controlling Federalization*, 75 N.Y.U. L. REV. 893, 910 (2000).

233. *See* Cobbledick v. United States, 309 U.S. 323, 325 (1940).

234. *See* Weeks v. United States, 232 U.S. 383 (1914) (finding a suppression remedy for violations of the Fourth Amendment); Wheeler v United States, 226 U.S. 478 (1913) (rejecting Fourth Amendment challenge to subpoena); Baltimore & Ohio R.R. v. Interstate Commerce Comm'n, 221 U.S. 612 (1911) (concluding that a federal administrative order requiring company to file reports with the agency did not violate the Fourth Amendment); Wilson v. United States, 221 U.S. 361 (1911) (rejecting Fourth Amendment challenge to subpoena); Hale v. Henkel, 201 U.S. 43 (1906) (articulating a Fourth Amendment standard for subpoenas); Adams v. New York, 192 U.S. 585 (1904); Brown v. Walker, 161 U.S. 591, 635 (1895) (Field, J., dissenting) (concluding in dictum that a federal law governing the production of witness violates the Fourth Amendment); Boyd v. United States, 116 U.S. 616 (1886) (concluding that the Fourth and Fifth Amendments block the use of a court order to compel a person to divulge their records); *Ex Parte* Jackson, 96 U.S. 727, 733 (1877) (concluding that the Fourth Amendment requires the government to obtain a warrant to open postal mail); Den v. Hoboken Land & Improvement Co., 59 U.S. (18 How.) 272, 286 (1855) (holding that a warrant of distress to levy on property of a collector of public revenues in default does not require the support of an oath or affirmation under the Fourth Amendment); *Ex Parte* Bollman, 8 U.S. (4 Cranch) 75, 110 (1807) (reviewing a warrant for probable cause).

235. The first cases that mention wiretapping by federal agents are *Wallace v. United States*, 291 F. 972 (6th Cir. 1923), *Wolf v. United States*, 292 F. 673 (6th Cir. 1923), and *Robilio v. United States*, 291 F. 975 (6th Cir. 1923). None of the cases are explicit about what kind of wiretapping occurred, however, or under what circumstances.

236. Craig S. Lerner, *The Reasonableness of Probable Cause*, 81 TEXAS L. REV. 951, 986 (2003) ("Long before the 'war on drugs,' the National Prohibition (or 'Volstead') Act provided an engine for the expansion of federal criminal law enforcement.").

237. Simons, *supra* note 232, at 911.

238. In 1917, Congress passed a statute codifying the common law process for obtaining search warrants. *See* Act of June 15, 1917, ch. 30, 40 Stat. 228 (repealed 1948). Section 3 of the Espionage Act provided, "A search warrant cannot be issued but upon probable cause, supported by affidavit, naming or describing the person and particularly describing the property and the place to be searched." *Id.*

to hear a regular run of Fourth Amendment cases as federal agents investigated illegal alcohol schemes.[240]

Federal law enforcement policy frowned upon wiretapping as a tool for investigating Prohibition crimes. Under the leadership of Attorney General (later Justice) Harlan Fiske Stone, the Justice Department banned the practice.[241] The nascent Federal Bureau of Investigations headed by J. Edgar Hoover supported this decision, and along with the Treasury Department opposed wiretapping entirely.[242] While there were sporadic reports of federal agents engaging in wiretapping in the early 1920s,[243] the first significant federal investigation in which wiretapping played a major role was also the first case to make it to the Supreme Court. That case was the investigation of Roy Olmstead.

The *Olmstead* case resulted from the decision of rogue officers from the federal Prohibition Office in Seattle to ignore the DOJ policy against wiretapping — and even the Washington state *law* against wiretapping — in order to catch local moonshine kingpin Roy Olmstead.[244] Olmstead was a former Seattle police officer who had bribed state and local officials and ran a massive Seattle-based

---

239. A Westlaw search for the number of times the phrase "search warrant" appeared in federal court decisions shows the impact of the change on the Fourth Amendment cases the courts evaluated. According to Westlaw's ALLFEDS-OLD database the phrase "search warrant" appears in the published opinions of U.S. courts the following number of times in particular years:

Year	Number of Cases including the Phrase "Search Warrant"
1905	1
1910	3
1918	10
1922	61
1925	114
1930	83

Source: ALLFEDS-OLD database, March 1, 2003.

240. A Westlaw search of the number of times that published federal court opinions included the phrase "Fourth Amendment" in different years produces the following results:

Year	Number of Cases including the Phrase "Fourth Amendment"
1905	1
1910	3
1918	7
1922	30
1925	40
1930	20

Source: ALLFEDS-OLD database, March 1, 2003.

241. MURPHY, *supra* note 79 at 13.

242. *See id.*

243. *See* cases cited in *supra* note 235.

244. *See* MURPHY, *supra* note 79, at 14.

operation to import alcohol.[245] To catch Olmstead, the Prohibition agents tapped the phone lines leading to his home and various business offices.[246] The agents then took notes of what they heard and later testified about it in court. Olmstead moved to suppress the evidence on the ground that wiretapping violated the Fourth Amendment — the first time the argument had ever been made in any court.[247] The district court rejected Olmstead's argument,[248] the jury convicted, and a divided Ninth Circuit affirmed.[249] Olmstead then petitioned the Supreme Court for a writ of certiorari, and the Supreme Court agreed to hear the case.[250]

Before the Supreme Court, the Justice Department offered only a half-hearted defense of the wiretapping investigation.[251] The investigation had been conducted by rogue agents in violation of both DOJ policy and state law; the case hardly presented federal law enforcement at its best.[252] At the same time, the stakes in *Olmstead* were quite high. A few years before *Olmstead*, the Supreme Court had ruled that the Fourth Amendment did not allow the government to obtain search warrants for "mere evidence"; the government could obtain warrants only to seize contraband, fruits of crime, or instrumentalities of crime.[253] Although the scope of the "mere evidence" rule was never entirely clear, it likely would have seemed at that time that wiretapping evidence would qualify as "mere evidence." As a result, the Fourth Amendment issue presented in *Olmstead* was probably all or nothing: either wiretapping did not implicate the Fourth Amendment at all, or else it violated the Fourth Amendment and the government could not wiretap even with a search warrant.

The Justice Department's cautious brief acknowledged that wiretapping violated DOJ policy, but argued that as a matter of constitutional law it did not violate the Fourth Amendment.[254] The

---

245. *See id.* at 15-17.

246. Olmstead v. United States, 277 U.S. 438, 456 (1928).

247. *Id.* at 456-57.

248. United States v. Olmstead, 7 F.2d 760, 763 (W.D. Wash 1925). In rejecting the argument, the trial judge reasoned that "[t]he conversation is not a property right. . . . I know of no rule of law or evidence which would exclude it, and no decision which, even by inference, sustains the contention of the defendant." *Id.*

249. Olmstead v. United States, 19 F.2d 842 (9th Cir. 1927). Judge Rudkin dissented. *See id.* at 848 (Rudkin, J., dissenting).

250. Olmstead v. United States, 277 U.S. 438 (1928), *cert. granted*, 276 U.S. 609 (1928)

251. *See* MURPHY, *supra* note 79, at 87.

252. *Cf. Olmstead*, 227 U.S. at 469 (Holmes, J., dissenting).

253. Gouled v. United States, 255 U.S. 298 (1921), *overruled by* Warden v. Hayden 387 U.S. 294, 308-309 (1967).

254. *See* MURPHY, *supra* note 79, at 87-88.

Supreme Court agreed by a 5-4 vote,[255] adopting the government's view that wiretapping from public property did not violate the Fourth Amendment because it did not physically trespass onto Olmstead's property.[256] Chief Justice Taft's opinion specifically invited Congress to pass a statutory protection against the admission of wiretapping evidence, but declined to impose such a rule as a constitutional matter:

> Congress may of course protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation, and thus depart from the common law of evidence. But the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment.[257]

B. *1934-1967: From the Communications Act to* Berger *and* Katz

The first permanent federal wiretapping law arrived just six years after Chief Justice Taft's invitation in *Olmstead*. In 1934, Congress passed the New Deal's Communications Act and included a provision prohibiting wiretapping, which was later codified at 47 U.S.C. § 605.[258] The law stated that "[n]o person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[259] The statute clearly made wiretapping a criminal offense, but the remedy was unclear.[260] In 1937, the Supreme Court interpreted the law to also serve an evidentiary function: according to the Court, the statute made all wiretapping evidence inadmissible in federal court.[261] The Court expanded that holding in 1939 to require the exclusion of "fruit of the poisonous tree" of illegal wiretapping.[262]

While this interpretation offered potentially expansive protection against wiretapping, its effectiveness was undercut dramatically by the Justice Department's interpretation of the law. Attorney General

---

255. Justices Holmes, Stone, Brandeis, and Butler dissented from the majority opinion. *See Olmstead*, 227 U.S. at 469-488.

256. *See id.* at 466 ("We think . . . that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.").

257. *Id.* at 465-66.

258. Sec. 605(a), 48 Stat. 1064, 1103-04 (1934).

259. 47 U.S.C. § 605(a) (2000).

260. *See, e.g.* United States v. Gruber, 123 F.2d 307 (2d Cir. 1941) (criminal prosecution brought under 47 U.S.C. § 605).

261. Nardone v. United States, 302 U.S. 379, 384 (1937).

262. Nardone v. United States, 308 U.S. 338, 341 (1939). This case introduced the "fruit of the poisonous tree" doctrine later adopted in the Fourth Amendment context. *See id.* ("[T]he trial judge must give opportunity, however closely confined, to the accused to prove that a substantial portion of the case against him was a fruit of the poisonous tree.").

(later Justice) Robert H. Jackson construed the statute as prohibiting the admission of wiretapping evidence in federal court, but *not* forbidding the wiretapping itself. Wiretapping was an "intercept," the Justice Department argued, but the statute prohibited the combination of intercepting and divulging or publishing the communication, which the Justice Department interpreted as disclosing outside law enforcement.[263] In a pre-*Bivens* era, the combination of the Supreme Court and Justice Department interpretations of the 1934 wiretapping law produced an odd legislative scheme. On one hand, the statute effectively overruled *Olmstead*: wiretapping evidence became flatly inadmissible in court, as was other evidence derived from the wiretapping.[264] On the other hand, the statute allowed wiretapping so long as the agents did not try to use the evidence in court.

State practices varied considerably during this period. Neither federal statutory nor constitutional rules applied to the states at the time: the federal ban applied only in federal court,[265] and the federal exclusionary rule did not apply to the states until 1961.[266] By 1967, however, the Supreme Court could survey the statutory law of wiretapping and conclude that "wiretapping on the whole is outlawed, except for permissive use by law enforcement officials in some states."[267] Thirty-six states had banned wiretapping.[268] Of those, twenty-seven allowed some type of "authorized" interception by law enforcement.[269] The most prominent law was New York's, passed in 1942.[270] New York's statute prohibited law enforcement wiretapping except pursuant to a search warrant signed by a judge.[271] During the late 1940s and early 1950s, the New York statute was used extensively by District Attorney Frank Hogan to wiretap and prosecute organized crime.[272]

---

263. Whether this interpretation was correct remains unclear. *See* AMERICAN BAR ASSOCIATION PROJECT ON MINIMUM STANDARDS FOR CRIMINAL JUSTICE, STANDARDS RELATING TO ELECTRONIC SURVEILLANCE 16 n.15 (1971).

264. United States v. Polakoff, 112 F.2d 888, 890 (2d Cir. 1940); Sablowsky v. United States, 101 F.2d 183 (3d Cir. 1938).

265. *See* Schwartz v. Texas, 344 U.S. 199, 203 (1952) ("We hold that § 605 applies only to the exclusion in federal court proceedings of evidence obtained and sought to be divulged in violation thereof; it does not exclude such evidence in state court proceedings.").

266. Mapp v. Ohio, 367 U.S. 643, 655 (1961) ("We hold that all evidence obtained by searches and seizures in violation of the Constitution is . . . inadmissible in a state court.").

267. Berger v. New York, 388 U.S. 41, 48-49 (1967).

268. *See id.* at 48 n.5.

269. *See id.* at 46.

270. *See* DASH ET AL., *supra* note 229, at 36.

271. *See id.* at 37-38.

272. *See id.* at 39-41.

The 1960s brought rumblings of change in wiretapping law from all three branches of government. In 1967, President Johnson's Crime Commission described the existing wiretapping law as "intolerable,"[273] noting that it was both overprotective and underprotective.[274] It was overprotective in that it did not allow federal agents to use wiretapping evidence in court at all, even against organized crime. On the other hand, the law offered no protection against wiretapping per se, allowing law enforcement to wiretap widely so long as they did not use the evidence in court. Congress became increasingly dissatisfied with the 1934 Communications Act. Bills to reform the wiretap laws had been introduced in every Congress but two since the *Olmstead* decision back in 1928, without success since 1934.[275] But by the mid-1960s, it became clear that comprehensive reform of federal wiretapping law was on the way. At the same time, the Warren Court repositioned itself to revisit *Olmstead*. In 1961, the Supreme Court ruled in *Mapp v. Ohio*[276] that the Fourth Amendment's suppression remedy now applied to the states.[277] This allowed the Court to reconsider how the Fourth Amendment applied to state wiretapping practices,[278] and in particular to determine whether wiretapping under the prominent New York wiretapping law satisfied the Fourth Amendment.

C. *1967 and 1968:* Berger, Katz, *and Title III*

The Supreme Court reviewed the New York state wiretapping statute just a few years after *Mapp*, in *Berger v. New York*,[279] granting a petition following a routine unpublished affirmance by New York's highest court.[280] *Berger* is unique among Fourth Amendment decisions in that the Court treated the case as a facial challenge to the New

---

273. PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 203 (1967) ("The present status of the law with respect to wiretapping and bugging is intolerable.").

274. *See id.* at 202-03.

275. *See* LONG, *supra* note 223, at 147.

276. 367 U.S. 643 (1961).

277. *Id.* at 655 (1961) ("We hold that all evidence obtained by searches and seizures in violation of the Constitution is . . . inadmissible in a state court.").

278. Before 1961, the Court had little opportunity to revisit *Olmstead*: wiretapping evidence was already inadmissible in federal court as a matter of statutory law, and although the Court held that the Fourth Amendment applied to the states in 1947, the suppression remedy did not apply. *See* Wolf v. Colorado, 338 U.S. 25, 33 (1949) (rejecting application of the Fourth Amendment's suppression remedy to state violations of the Fourth Amendment).

279. The Supreme Court granted the petition for certiorari in the case on December 5, 1996. *See* 385 U.S. 967-68 (1966).

280. *See* People v. Berger, 18 N.Y.2d 638 (1966), *rev'd sub nom.* Berger v. New York, 388 U.S. 41 (1967).

York statute.[281] The Supreme Court did not answer the usual question of whether the government had violated the defendant's Fourth Amendment rights.[282] Instead, the Court took the *Berger* case as an opportunity to examine the various components of the New York statute and explain which of them were constitutional and which were not. The *Berger* opinion tells us that to be constitutional, a wiretapping law must require: a) that "a neutral and detached authority" evaluate whether probable cause exists before wiretapping occurs;[283] b) that the application for the court order to explain "[w]hat specific crime has been or is being committed," "the place to be searched," and "the persons or things to be seized";[284] c) that the order authorizing the wiretapping "places a termination date" on the surveillance;[285] d) that there is "notice as [with] conventional warrants," or "some showing of special facts" to excuse notice;[286] and e) "a return on the warrant."[287] Because New York's statute did not have all of these requirements, the Supreme Court struck it down.[288]

What explains the unusual facial challenge in *Berger*? Awareness of Congress's keen interest in revising the federal wiretapping laws is one explanation. As Justice White noted in his dissent, at the time of *Berger* Congress was in the midst of holding "extensive hearings"[289] before both the House and Senate Judiciary Committees on how to rewrite the wiretap laws along the lines of New York's law.[290] Justice White noted that Congress was waiting to find out what kind of wiretapping law the Court might allow. "The grant of certiorari in this case has been widely noted," Justice White explained, "and our decision can be expected to have a substantial impact on the current

281. *See Berger*, 388 U.S. at 90-91 (Harlan, J., dissenting) (noting the majority's unexplained decision to treat the case as a facial challenge, rather than as an as-applied challenge).

282. *See id.*

283. *Id.* at 54.

284. *Id.* at 58-60.

285. *Id.* at 59.

286. *Id.* at 60.

287. *Id.*

288. *See id.* at 64. Notably, the Supreme Court also eliminated the "mere evidence" rule in *Warden v. Hayden*, 387 U.S. 294 (1967), decided just two weeks before *Berger* was announced. *Hayden* was decided on May 29; *Berger* was announced on June 12. With *Hayden* overruled, the Court could allow a warrant for "mere evidence of wiretapping."

289. *Berger*, 388 U.S. at 112 (White, J., dissenting) ("Bills have been introduced at this session of Congress to fill this legislative gap, and extensive hearings are in progress before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, and before Subcommittee No. 5 of the House Committee on the Judiciary.").

290. *See id.*

legislative consideration of these issues."[291] President Johnson's influential Crime Commission report had advised as much: the Commission urged Congress to enact new wiretap laws on the New York model, but urged that "any congressional action should await the outcome"[292] of the then-pending *Berger* case.

Berger was not the only decision that Congress was waiting for the Supreme Court to decide. The Court had granted certiorari in *Katz v. United States* one month before oral argument in *Berger*.[293] Importantly, *Katz* was not another wiretapping case: the surveillance in that case involved a microphone taped to the top of a phone booth.[294] Commentators often overlook this because the Supreme Court's description of the facts seems almost intentionally vague; while the Ninth Circuit opinion explained that the FBI in *Katz* had merely taped a microphone to the top of the booth,[295] the Supreme Court wrote ambiguously that the FBI had "attached an electronic listening and recording device"[296] to the booth. In any event, by evaluating a bugging case as well as a wiretapping case, the Court made clear that it would consider both prominent forms of surreptitious surveillance roughly at the same time — and that Congress would have to wait for both. Like Berger, *Katz* revealed a legislative orientation; in his otherwise harsh dissent, Justice Black complimented the majority for its "good efforts" to articulate "methods in accord with the Fourth Amendment to guide States in the enactment and enforcement of laws passed to regulate wiretapping by government."[297]

Far from being sui generis constitutional developments, the major constitutional decisions in *Berger* and *Katz* were carefully timed to influence the shape of statutory law. The Court was eyeing Congress, and decided both *Berger* and *Katz* very much with Congress in mind.

---

291. *Id.* at 113.

292. PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, *supra* note 273, at 203.

293. The order granting the petition for a writ of certiorari in *Katz* is noted at 386 U.S. 954-55 (1967). *Berger* was argued on April 13, 1967. *See* 388 U.S. 41 (1967).

294. Katz v. United States, 369 F.2d 130, 131 (9th Cir. 1966).

295. The Ninth Circuit explained the facts as follows:

> In the period of February 19 to February 25, 1965, at set hours, Special Agents of the Federal Bureau of Investigation placed microphones on the tops of two of the public telephone booths normally used by the appellant. The other phone was placed out of order by the telephone company. The microphones were attached to the outside of the telephone booths with tape. There was no physical penetration inside of the booths. The microphones were activated only while appellant was approaching and actually in the booth. Wires led from microphones to a wire recorder on top of one of the booths. Thus the F.B.I. obtained a record of appellant's end of a series of telephone calls.

Katz, 369 F.2d at 131.

296. *Katz*, 389 U.S. at 348.

297. *See Id.* at 364 (Black, J., dissenting).

Senator McClellan had introduced S. 675, the Federal Wire Interception Act, a few months before *Berger* on January 25, 1967.[298] Two weeks after *Berger*, Senator Hruska introduced S. 2050, the Electronic Surveillance Control Act, which incorporated *Berger*'s teachings.[299] S. 675 and S. 2050 were then modified to comply with *Katz* in December 1967 and together formed the basis of the legislation that Congress ultimately passed in June 1968.[300] Since 1968, the Federal Wiretap Act has been the governing wiretapping law in the United States.[301] It is often referred to as "Title III" because it passed as the third section of the mammoth Omnibus Crime Control Act of 1968.[302] The Senate Report that accompanied Title III made clear that Congress had taken the existing proposals and reformulated them to comply with *Berger* (for wiretapping) and *Katz* (for bugging).[303]

D. *Wiretapping After Title III: Constitutional in Theory, Statutory in Fact*

The history now brings us to the modern era, the period after *Katz*, *Berger*, and the passage of Title III. In this period, as in previous ones, statutory protections rather than constitutional protections provide the driving force behind wiretapping law. *Berger* and *Katz* remain on the books, of course, but wiretapping law is largely statutory in practice. Fourth Amendment decisions regulating wiretapping remain notably rare. When confronted with claims that wiretapping violated the Fourth Amendment, courts typically fall back on the statutory protections of Title III and go no further.

The judiciary's deferential stance began with the case law that followed the passage of Title III. Defendants tried to challenge Title III on the same facial grounds used successfully in *Berger*, but these

---

298. *See* S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153.

299. *See id.*

300. *See id.*

301. *See* 18 U.S.C. §§ 2510-22 (2000).

302. Pub. L. 90-351, 82 Stat. 197 (1968).

303.

> Title III prohibits all wiretapping and electronic surveillance by persons other than duly authorized law enforcement officials engaged in the investigations of specified types of major crimes after obtaining a court order, with exceptions provided for interceptions by employees of communications facilities whose normal course of employment would make necessary such interception, personnel of the Federal Communications Commission in the normal course of employment, and government agents to secure information under the powers of the President to protect the national security. This proposed legislation conforms to the constitutional standards set out in Berger v. New York, 388 U.S. 41 (1967), and Katz v. United States, 389 U.S. 347 (1967). See 1968 U.S.C.C.A.N. at 2113.

1968 U.S.C.C.A.N. 2112, 2113.

claims were universally rejected.[304] The formidable statutory privacy protections found in the Wiretap Act are no doubt responsible for some of this. Consider the case of a wiretap order to tap a telephone line. Before applying for a court order to tap the line, federal prosecutors must:

1) obtain high-level Justice Department approval under Section 2516(1);
2) show that the wiretapping will be used to uncover evidence of one of the predicate felony offenses listed in Section 1516(1)(a)-(r);
3) author an application supported by a "full and complete statements of the facts," a particular description of the nature and location of the place where the communication will be intercepted, and, if known, the identity of the persons whose communications will be intercepted, all under Section 2518(b);
4) show that the wiretapping was necessary because "other investigative procedures have been tried and failed," or else reasonably appear unlikely to succeed, under Section 2511(2)(c);
5) offer the court a full and complete statement of the facts concerning all previous related wiretap applications under 2511(2)(d);
6) show probable cause that interception of the calls under a wiretap order will yield communications concerning the criminal offense under Section 2518(3)(b); and
7) explain to the court the mechanism that the government will use to minimize the interception of communications unrelated to the criminal investigation pursuant to Section 2518(5).

Nor do the statutory obligations end once the order is signed by the federal district court judge. The government must file regular reports to the issuing judge (typically at ten day intervals) explaining "what progress has been made toward achievement of the authorized objective" and justifying the need for further wiretapping under Section 2516(6). The wiretapping cannot last for "longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days" under Section 2518(5). Immediately

304. *See, e.g.*, United States v. Sklaroff, 506 F.2d 837, 840 (5th Cir 1975); United States v. Ramsey, 503 F.2d 524, 526-31 (7th Cir. 1974); United States v. Martinez, 498 F.2d 464, 467-68 (6th Cir. 1974); United States v. Tortorello, 480 F.2d 764, 771-75 (2d Cir. 1973); United States v. Bobo, 477 F.2d 974, 978-82 (4th Cir. 1973); United States v. Whitaker, 474 F.2d 1246, 1247 (3d Cir. 1973); United States v. Cafero, 473 F.2d 489, 493-501 (3d Cir. 1973); United States v. Cox, 449 F.2d 679, 683-87 (10th Cir. 1971).

after the wiretapping has been completed, the records of the wiretapping must be made available to the issuing judge and sealed and kept for ten years under Section 2516(8). Within ninety days after the surveillance has ended, the subjects of the wiretapping (and at the discretion of the issuing judge, others known to have had their conversations recorded) must be notified that they were tapped and when, pursuant to Section 2518(8)(d). Finally, the basic facts about the order must be included in an annual report filed by the Justice Department and made available to the public under Section 2519. If state agents want to wiretap, they must comply not only with the usual federal rules, but also with additional federal rules that impose special restrictions on state practices, and state rules that are often much more restrictive than federal rules.[305]

Like any legislation, Title III has gaps and weaknesses. But despite *Berger* and *Katz*, courts have proved surprisingly reluctant to find that the occasional holes in the Wiretap Act violate the Fourth Amendment. Consider the cases involving the wiretapping of cordless phone calls. Before 1994, Congress chose not to extend the protections of the Wiretap Act to cordless telephone calls;[306] "the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base"[307] was expressly exempted from the statute. This decision created a curious statutory anomaly; conversations on land-line phones were protected by the Wiretap Act while conversations on cordless phones were not. But the courts refused to say that the Fourth Amendment covered the ground that Congress had not protected: instead, the courts deferred to Congress's judgment and held that such calls were not covered by the Fourth Amendment.[308] The Fourth Circuit even used the occasion to warn against the dangers of fashioning Fourth Amendment privacy rights in new technologies given Congress's statutory framework:

> In the fast-developing area of communications technology, courts should be cautious not to wield the amorphous "reasonable expectation of privacy" standard, in a manner that nullifies the balance between privacy

---

305. *See generally* Charles H. Kennedy & Peter P. Swire, *State Wiretaps and Electronic Surveillance After September 11*, 54 HASTINGS L.J. 971 (2003).

306. *See* McKamey v. Roach, 55 F.3d 1236, 1238 n.1 (6th Cir. 1995) (noting that Congress did not protect cordless telephone calls via Title III until it passed the Communications Assistance for Law Enforcement Act, Pub.L. No. 103-414, § 202(a), 108 Stat. 4279 (1994)).

307. 18 U.S.C. § 2510(1) (1988), *repealed by* Pub.L. No. 103-414, § 202(a), 108 Stat. 4279 (1994).

308. *See McKamey*, 55 F.3d at 1239-40; Tyler v. Berodt, 877 F.2d 705, 707 (8th Cir. 1989) (involving a call from a cordless phone); United States v. McNulty (*In re* Askin), 47 F.3d 100, 104-106 (4th Cir. 1995) (involving a call made to a cordless telephone user); United States v. Smith, 978 F.2d 171, 177-81 (5th Cir. 1992); Price v. Turner, 260 F.3d 1144, 1149 (9th Cir. 2001).

> rights and law enforcement needs struck by Congress in Title III .... As new technologies continue to appear in the marketplace and outpace existing surveillance law, the primary job of evaluating their impact on privacy rights and of updating the law must remain with the branch of government designed to make such policy choices, the legislature. Congress undertook in Title III to legislate comprehensively in this field and has shown no reluctance to revisit it. Accordingly, we must decline [the defendant]'s invitation to usher in through the Fourth Amendment a prohibition of that which Title III tells us, in no uncertain terms, Congress affirmatively permitted at the time this case arose.[309]

The same posture of judicial restraint led the Sixth Circuit to rule that plaintiffs cannot raise civil claims under the Fourth Amendment for illegal wiretapping, and that only statutory claims under Title III are allowed.[310] In *Adams v. City of Battle Creek*,[311] a city police officer sued the city under both the statutory Wiretap Act and the Fourth Amendment for wiretapping his department-issued pager.[312] On appeal, the Sixth Circuit concluded that the "detailed legislative scheme"[313] of the Wiretap Act should "provide the exclusive remedies in the field"[314] of wiretapping law. The availability of statutory civil remedies under Title III foreclosed a civil remedy under the Fourth Amendment. According to the court, the Wiretap Act

> seeks to balance privacy rights and law enforcement needs, keeping in mind the protections of the Fourth Amendment against unreasonable search and seizure. Congress made the Act the primary vehicle by which to address violations of privacy interests in the communication field" ... Because no argument is made that the substantive or remedial standards provided by the Fourth Amendment differ from the federal statute, we do not reach any question of interpretation under the Fourth Amendment. All such constitutional issues are pretermitted.[315]

In other words, the existence of the statutory Wiretap Act effectively displaces any constitutional remedies that in theory should exist under cases like *Katz* and *Berger*.

Courts have shown similar deference to statutory law in areas beyond the Wiretap Act's core concern of domestic wiretapping in criminal cases. For example, courts occasionally encounter cases in which U.S. government agents wiretap U.S. citizens overseas, beyond

309. *McNulty*, 47 F.3d at 105-06 (internal citations omitted).

310. Adams v. City of Battle Creek, 250 F.3d 980, 986 (6th Cir. 2001).

311. 250 F.3d 980 (6th Cir. 2001).

312. *See id.* at 980.

313. *Id.* at 986.

314. *Id.*

315. *Id.*

the territorial scope of the Wiretap Act,[316] often jointly with the governments of foreign countries.[317] In the bulk of these cases, the courts have deferred to statutory standards abroad; courts have held that Fourth Amendment reasonableness hinges on whether the wiretapping complied with statutory law of the foreign country where the wiretapping occurred.[318]

The same deference to legislative standards appears in cases exploring how the Fourth Amendment applies to covert video surveillance specifically exempted from the Wiretap Act. Rather than create new judicial standards from scratch, courts have held that the Fourth Amendment is satisfied if the government complies with equivalent statutory standards that Title III enacted to regulate audio wiretapping. When called to formulate Fourth Amendment standards in areas that Congress has left unregulated, courts have set them by adopting the nearest statutory requirements.[319] Even when the Supreme Court held that the Fourth Amendment applied to domestic wiretapping conducted for national security reasons, the Court specifically called on Congress to enact a new statute to set up the legal standards.[320]

---

316. *See* United States v. Toscanino, 500 F.2d 267, 279 (2d. Cir. 1974) (noting that the Wiretap Act does not apply outside the United States).

317. *See, e.g.*, United States v. Peterson, 812 F.2d 486, 490 (9th Cir. 1987); United States v. Barona, 56 F.3d 1087, 1093-95 (9th Cir. 1995).

318. *See, e.g.*, *Peterson*, 812 F.3d at 490 ("If, however, United States agents' participation in the investigation is so substantial that the action is a joint venture between United States and foreign officials, the law of the foreign country must be consulted at the outset as part of the determination whether or not the search was reasonable.").

319. Ric Simmons has criticized this practice in the context of video surveillance. *See* Simmons, *supra* note 218, at 589. Simmons charges that the courts "have relinquished their judicial duty to interpret the Constitution, an abdication which . . . is especially problematic when it occurs in the context of surveillance techniques that are both extraordinarily intrusive and becoming more common and more technologically sophisticated every year." *Id.*

320. In 1972, the Supreme Court ruled that the *Katz* rationale applied to domestic surveillance in national security cases, not merely the criminal cases regulated by Title III. United States v. United States District Court, 407 U.S. 297 (1972). Once again the Court offered extensive statutory guidance to Congress. The Court wrote:

> Given those potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. . . .
>
> It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of § 2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court (e.g., the District Court for the District of Columbia or the Court of Appeals for the District of Columbia Circuit); and that the time and reporting requirements need not be so strict as those in § 2518.
>
> The above paragraph does not, of course, attempt to guide the congressional judgment but rather to delineate the present scope of our own opinion. We do not attempt to detail the precise standards for domestic security warrants any more than our decision in *Katz* sought

As these cases suggest, wiretapping law may be constitutional in theory, but it is statutory in practice. For prosecutors and defense attorneys, complying with wiretapping law means complying with statutory law; challenging wiretapping practices means challenging practices on statutory grounds. When wiretapping occurs inside the United States, courts generally refuse to construe the Fourth Amendment as going beyond the scope of the Wiretap Act; when wiretapping occurs outside the United States, courts often equate the Fourth Amendment with compliance with foreign statutory law. *Berger* and *Katz* helped shape the statutory structure at the time of the key statute's enactment. But despite their impact, the sources of wiretapping law have remained largely statutory.

E. *Privacy in New Technologies and the Statutory Norm*

Wiretapping is not an exception to the rule. A broader look at the legal standards that govern criminal investigations involving new technologies suggests that Congress has often taken the lead, and that judicial decisions interpreting the Fourth Amendment generally have played a secondary role. In some instances, congressional action has followed Supreme Court decisions interpreting the Fourth Amendment. For example, the Court's decision in the *Keith* case considering how the Fourth Amendment applies to national security wiretapping helped inspire the passage of the Foreign Intelligence Surveillance Act in 1978. The Court's conclusion in *Smith v. Maryland*[321] that the Fourth Amendment did not protect numbers dialed from a telephone (so-called "pen register" information)[322] led Congress to protect such information in 1986, via the Pen Register and Trap and Trace Devices Statute.[323]

Congress has also acted on its own initiative to protect privacy against the threat of new technology. For example, Congress passed the Privacy Act of 1974[324] to give citizens the right to check and correct information about themselves in government computer databases.[325] Congress protected the privacy of cable television subscribers by passing strict restrictions against the disclosure of their personal

---

to set the refined requirements for the specified criminal surveillances which now constitute Title III. We do hold, however, that prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.

Id. at 322-24.

321. 442 U.S. 735 (1979).

322. *See id.* at 742.

323. 18 U.S.C. §§ 3121-27 (2000). *See generally* Kerr, *Internet Surveillance, supra* note 161 (discussing the Pen Register statute).

324. Pub. L. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a (2000)).

325. *See generally* Laurie A. Doherty, *Privacy Act*, 56 GEO. WASH. L. REV. 1028 (1988).

information in the Cable Communications Privacy Act of 1984.[326] Two years later, Congress protected the privacy of stored e-mails and Internet communications by passing the Electronic Communications Privacy Act.[327] Two years after that, Congress passed the Video Privacy Protection Act[328] to protect the privacy of video store customers.

Congress has also passed privacy laws outside of the high technology area, often in response to developments in Fourth Amendment law. Congress enacted the Right to Financial Privacy Act[329] to protect the privacy of bank records after the Supreme Court ruled that the Fourth Amendment did not protect such records in 1976.[330] Congress created the Privacy Protection Act of 1980[331] to offer the press special protections against searches and seizures after the Supreme Court declined to do so in a 1978 case.[332] And this list is not exhaustive; other federal statutory privacy laws exist.[333]

Of course, the legislative enactment of law enforcement regulations beyond the Fourth Amendment does not necessarily mean that these statutory laws are adequate. I have argued both in congressional testimony and in my academic writing that Congress's handiwork in the field of Internet surveillance law offers a promising framework, but needs reforms to bolster privacy protections.[334] At the same time, Congress's track record is often ignored by scholars even

---

326. Cable Communications Privacy Act, 47 U.S.C. § 551 (2000). *See* Doherty, *supra* note 325.

327. Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq.* (2000).

328. Video Privacy Protection Act, 18 U.S.C. § 2710 (2000); Pub. L. 100-618, § 2(a)(2), 102 Stat. 3195 (1988).

329. Right to Financial Privacy Act, 12 U.S.C. §§ 3401-22 (2000); Pub. L. 95-630, 92 Stat. 3697 (1978).

330. United States v. Miller, 425 U.S. 435, 443 (1976).

331. Privacy Protection Act, 42 U.S.C. § 2000aa (2000). For a comprehensive discussion of the Privacy Protection Act, *see* UNITED STATES DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 61-69 (2002).

332. *See* Zurcher v. Stanford Daily, 436 U.S. 547 (1978).

333. For as more comprehensive list, see MARC ROTENBERG & DANIEL SOLOVE, INFORMATION PRIVACY LAW 23-24 (2003).

334. *See, e.g.*, *Anti-Terrorism Investigations and the Fourth Amendment After September 11, 2001, Hearing Before the House Judiciary Committee Subcommittee on the Constitution*, 108th Cong. 26 (2003) (statement of Orin S. Kerr) (arguing that Congress should raise the standard that the government needs to satisfy to obtain a pen register order); Kerr, *Internet Surveillance Law After the USA Patriot Act*, *supra* note 161; Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How A Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805 (2003) [hereinafter Kerr, *Lifting the "Fog"*] (arguing that Congress should add a suppression remedy for violations of the Internet surveillance statutes); Orin S. Kerr, *A User's Guide to the Stored Communications Act — And a Legislator's Guide to Amending It*, GEO. WASH. L. REV. (forthcoming 2004) (arguing that Congress should raise the thresholds in 18 U.S.C. 2703(b) to better protect privacy).

when statutes provide the most important privacy protection against invasive government practices.[335] Both criminal procedure and privacy law scholars have tended to focus their attention on the Fourth Amendment, overlooking the reality that since the 1960s Congress rather than the courts has shown the most serious interest in protecting privacy from new technologies. Judicial decisions have played a role by shaping legislation, but the real work that has been done to regulate law enforcement use of new technologies has come primarily from Congress, not the courts.

III. INSTITUTIONAL COMPETENCE AND REGULATION OF GOVERNMENT INVESTIGATIONS INVOLVING NEW TECHNOLOGIES

I have argued in this Article that both the history of the Fourth Amendment and existing doctrine counsel against expansive interpretations of the Fourth Amendment in developing technologies. Up to now, however, I have not addressed the related normative questions. In this Section, I will address one important normative inquiry generally answered in the affirmative by proponents of the popular view. Assuming Fourth Amendment doctrine or theory renders judicial rulemaking in new technologies necessary, are courts institutionally equipped to regulate new technologies effectively? By corollary, should courts approach the task with confidence or caution?

Proponents of broad Fourth Amendment protection generally believe that courts are well equipped to create effective privacy rules.[336] If technology threatens privacy, the best source of new privacy protections are the judiciary rather than legislatures.[337] Professor

335. For example, in his work *Code and Other Laws of Cyberspace*, Professor Lessig considers a variety of ways in which new technologies may threaten how the Fourth Amendment protects privacy. *See* LESSIG, *supra* note 10, at 144-46. Lessig acknowledges that statutory protections against such privacy invasions exist and "are in fact quite rich," but quickly moves on to constitutional questions. *Id.*

336. *See, e.g.*, 1 LAFAVE ET AL., CRIMINAL PROCEDURE § 2.1 (2d ed. 1999) (arguing that the courts are well equipped to regulate criminal procedure rules because courts understand the criminal process and are not subject to political pressures to deny basic liberties); Donald A. Dripps, Essay, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; Or, Why Don't Legislatures Give a Damn About the Rights of the Accused?*, 44 SYRACUSE L. REV. 1079 (1993) (arguing that legislatures do not enact criminal procedure laws that protect the rights of the accused because they face political pressures to punish and deter crime).

337. *See, e.g.*, Blitz, *supra* note 7, at 1420-1423 (arguing that courts are able "to judge when the surveillance schemes involved in a particular dispute leave citizens with too little privacy."); Nola K. Breglio, Note, *Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 Yale L.J. 179, 215 (2003) ("When a statutory [surveillance] regime is failing, better that we leave it behind, return directly to the document the Framers handed us, and charge our judges with adapting their words to our modern circumstances."); *Cf.* William J. Fenrich, Note, *Common Law Protection Of Individuals' Rights In Personal Information*, 65 FORDHAM L. REV. 951, 986-90 (1996) (arguing that the courts are best equipped to create rules protecting personal privacy).

Lessig offers such a perspective in his book *Code and Other Laws of Cyberspace*. Lessig urges judges to be bold in their use of the Fourth Amendment to protect Internet privacy: he writes that "judges should firmly advance arguments that seek to preserve original values of liberty in a new context."[338] Because the Fourth Amendment reflects a clear commitment of the Framers to protect privacy,[339] judges should identify the values of privacy in new technologies and translate them in to new Fourth Amendment rules.[340] Lessig singles out Justice Brandeis's *Olmstead* dissent as a model for how to interpret the Fourth Amendment in light of technological change: "If there is a justice who deserves c-world's praise, if there is a Supreme Court opinion that should be the model for cyberactivists in the future, if there is a first chapter in the fight to protect cyberspace, it is this Justice, this opinion, and this case."[341] If courts defer to legislatures, Lessig warns, we will be left with laws that may or may not respect constitutional values.[342] Thus "there is an important space for [judicial] activism."[343] Professor Lessig suggests that lower court judges should act with particular confidence; "many [lower court judges] are extraordinarily talented and creative. Their voices would teach us something. . . ."[344]

In this part, I will argue that such enthusiasm for judicial solutions overlooks significant institutional limitations of judicial rulemaking. Courts tend to be poorly suited to generate effective rules regulating criminal investigations involving new technologies. In contrast, legislatures possess a significant institutional advantage in this area over courts. While courts have successfully created rules that establish important privacy rights in many areas, it is difficult for judges to fashion lasting guidance when technologies are new and rapidly changing. The context of judicial decisionmaking often leaves the law surprisingly unclear. Courts lack the institutional capacity to easily grasp the privacy implications of new technologies they encounter. Judges cannot readily understand how the technologies may develop, cannot easily appreciate context, and often cannot even recognize

338. LESSIG, *supra* note 10, at 222.

339. *Id.* at 117-18.

340. *Id.* at 222.

341. *Id.* at 116.

342. Lessig writes that as courts notice how their decisions may influence the development of the Internet, "they will increasingly defer to the political branches." *Id.* at 216. "[W]e should not underestimate" the consequences of such deference, he warns: "In the future legislatures will act relatively unconstrained by courts; the values that we might call constitutional — whether enacted into our Constitution or not — will constrain these legislatures only if they choose to take them into account." *Id.*

343. *Id.* at 222.

344. *Id.*

whether the facts of the case before them raise privacy implications that happen to be typical or atypical. Judicially created rules also lack necessary flexibility; they cannot change quickly and cannot test various regulatory approaches. As a result, judicially created rules regulating government investigations tend to become quickly outdated or uncertain as technology changes. The context of legislative rule-creation offers significantly better prospects for the generation of balanced, nuanced, and effective investigative rules involving new technologies. In light of these institutional realities, courts should proceed cautiously and with humility, allowing some room for political judgment and maneuvering in a setting that is in such flux.[345]

My argument here is relatively narrow, and two major limitations are worth stating at the outset. First, my normative argument is limited to the field of criminal procedure, and particularly the Fourth Amendment. Civil law scholars have noted that courts have two significant institutional advantages over legislatures when technology is in flux. First, courts can generate rules in a case-by-case way that may offer significant advantages over one-size-fits all legislative solutions, especially when technologies are new and may change.[346] Second, legislative rules are subject to rent-seeking by special interest groups, while judicial decisionmaking tends to be more independent.[347] As I explain in greater detail later in the section, I find both arguments persuasive in the civil law context. The dynamic of criminal procedure is different, however. In the latter context, interstitial decisionmaking proves more a liability than an asset because the rules govern law enforcement, not private parties. Uncertain rules result in uncertain restrictions on government practices, which can either allow abuses or else chill practices needed to pursue important investigations. Further, privacy rules present relatively few opportunities for rent-seeking, and instead tend to produce strong incentives for legislators to enact rules that reflect majority preferences.

The second limitation is that my argument applies only when technologies are in flux. My concern is the institutional competence of courts and legislatures when facts are changing quickly. As a result, my interest is not whether a given case involves a "technology" in an absolute sense, but rather whether the basic assumptions upon which rules are generated are likely to remain constant or to shift in unpredictable ways. The argument thus has a significant temporal aspect; it is not an argument against strong Fourth Amendment protection, but rather an argument for judicial caution in the face of rapid technological change. When technologies are new and their impact remains uncertain, statutory rules governing law enforcement

345. Cass R. Sunstein, *Constitutional Caution*, 1996 U. CHI. LEGAL F. 361, 363.

346. *See infra* notes 485-494.

347. *See infra* notes 497-498.

powers will tend to be more sophisticated, comprehensive, forward-thinking, and flexible than rules created by the judicial branch. The temporal limitation also responds to concerns that legislatures may enact rules that dismiss privacy concerns. Because early adopters of new technologies tend to have disproportionate political influence, legislators often will be unusually sensitive to privacy threats raised by technological change.

A. *Judicial Creation of Investigative Rules When Facts Are Stable*

During the Warren Court era, scholars of criminal procedure debated the Court's constitutionalization of criminal procedure. For the most part, the debate focused on the merits of the Court's decisions as exercises in constitutional interpretation.[348] Some found the Court's criminal procedure cases well-meaning but poorly reasoned and results-oriented; others argued that the decisions courageously fulfilled the promise of the Bill of Rights.[349] Whatever the merits of these arguments, it is difficult to contest the fact that over the last forty years the Court has constitutionalized the law governing criminal investigations. Today, the law of criminal procedure is mostly constitutional law.[350] Although some criticize the Supreme Court's rules as ineffective and unworkable,[351] I think the Supreme Court's rules by and large have worked. The rules provide reasonably clear guidance to law enforcement, limit government power to protect privacy (within limits), and give the police enough authority to protect public safety (again, within limits).[352] Although no one could agree entirely with the Court's work, from a functional perspective most of the Court's Fourth Amendment decisions are part of a reasonably coherent and sensible rule structure.

The fact that the Supreme Court has successfully used the Fourth Amendment in the past to create rules governing law enforcement investigations prompts an important question: If the Court has succeeded in constitutionalizing the basic rules governing criminal

348. *But see* Paul M. Bator & James Vorenberg, *Arrest, Detention, Interrogation and the Right to Counsel: Basic Problems and Possible Legislative Solutions*, 66 COLUM. L. REV. 62, 62-63 (1966).

349. *See, e.g.*, Henry J. Friendly, *The Bill of Rights as a Code of Criminal Procedure*, 53 CAL. L. REV. 929 (1965).

350. 1 LAFAVE ET AL., *supra* note 336, § 2.1 at 469 ("Looking to the totality of the [criminal] process, constitutional standards combine to constitute what is surely the single most important body of law regulating the process.").

351. *See* CRAIG M. BRADLEY, THE FAILURE OF THE CRIMINAL PROCEDURE REVOLUTION (1993) (arguing that case-by-case decisionmaking leaves criminal procedure rules unclear, and that Congress should enact a federal code of criminal procedure to provide clear rules for the police to follow).

352. *See infra* notes 353-357.

investigations, why can't courts do the same in cases with new technologies? What changes when we shift to cases with technologies in flux? This Part explores the characteristics of traditional cases that have allowed the courts to develop privacy laws that regulate them. By appreciating why courts can devise rules effectively in traditional cases, we can then understand why that ability diminishes in cases with developing technologies.

Let's begin with the goals of Fourth Amendment rules. It is generally agreed that the general pragmatic goal of both constitutional and statutory law governing search and seizure is to create a workable and sensible balance between law enforcement needs and privacy interests.[353] The law should allow the government to investigate crime effectively, facilitating the substantive goals of criminal law such as deterrence and retribution. At the same time, the law must limit the power of government, in order to protect privacy and civil liberties against excessive government snooping. These general goals of course mask a great deal of disagreement on the specifics; lines can be drawn in different places, and different people have different views as to how this balance should be reached. But at least at a more abstract level, the goal is a rule-structure that simultaneously respects privacy interests and law enforcement needs.

A secondary goal is rule clarity. The rules of criminal procedure primarily regulate law enforcement instead of private parties; the rules tell government agents what they can and cannot do to collect evidence of crime and identify wrongdoers. Because these rules limit government power, rule clarity minimizes official discretion and encourages compliance.[354] Unclear rules mean unclear limits on government power, increasing the likelihood of abuses by aggressive government officials.[355] Clear rules also limit the shield of qualified

353. *See, e.g.*, Illinois v. McArthur, 531 U.S. 326, 330 (2001)

354. For example, this is the purpose of the Fourth Amendment's particularity requirement: by requiring officers to explain with particularity what exactly they want to seize pursuant to a warrant, the particularity requirement limits the discretion of officers who may otherwise use the warrant as an excuse to engage in a fishing expedition for evidence of criminal activity. *See* Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (discussing the function of the particularity requirement); Marron v. United States, 275 U.S. 192, 196 (1927) ("As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").

355. As the Supreme Court has noted, Fourth Amendment rules:

> [O]ught to be expressed in terms that are readily applicable by the police in the context of the law enforcement activities in which they are necessarily engaged. A highly sophisticated set of rules, qualified by all sorts of ifs, ands, and buts and requiring the drawing of subtle nuances and hairline distinctions, may be the sort of heady stuff upon which the facile minds of lawyers and judges eagerly feed, but they may be "literally impossible of application by the officer in the field . . . .
>
> [A] single, familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront."

immunity, increasing deterrence.[356] From a public safety perspective, clear rules also allow investigators to use the full power granted to them under constitutional and statutory law to pursue evidence of criminal activity.[357]

Both goals are readily attainable through judicially crafted rules when technologies are stable. Consider automobile traffic stops, one of the most common fact patterns in Fourth Amendment law. In these cases, the police spot a vehicle on a public road and wish to stop the car and investigate further. Stopping the car is plainly a Fourth Amendment "seizure,"[358] focusing attention on the line between a "reasonable" and an "unreasonable" seizure — and if a search of the vehicle later occurs, a "reasonable" and an "unreasonable" search. What can the police do? What rules exist to balance law enforcement needs with privacy interests?

The Supreme Court has developed a remarkably detailed set of rules that govern every stage of traffic stops. The officer can stop the car if he has probable cause to believe that the driver has committed a traffic violation, no matter how minor.[359] At that point, he can order the driver and the passengers out of the car.[360] If the officer has reasonable suspicion that the driver is armed and dangerous, he can "patdown" the driver, and search the passenger compartment of the vehicle. Otherwise he cannot.[361] The officer can look through the windows of the vehicle,[362] and if he has probable cause to search the vehicle, he can search it without a warrant,[363] looking anywhere that evidence may be located.[364] If the driver or someone else with common authority consents, he can search the vehicle within the scope of that

---

New York v. Belton, 453 U.S. 454, 458 (1981) (quoting Wayne R. LaFave, *"Case-by-Case Adjudication" versus "Standardized Procedure": The* Robinson *Dilemma*, 1974 S. CT. REV. 127, 142 (quoting United States v. Robinson, 471 F.2d 1082, 1122 (Wilkey, J., dissenting) (1972), and quoting Dunaway v. New York, 442 U.S. 200, 213-14 (1979))).

356. When the state of the law is unclear, law enforcement officers are generally protected from civil suits by the doctrine of qualified immunity. *See* Anderson v. Creighton, 483 U.S. 635, 640 (1987).

357. *See* Kerr, *Lifting the "Fog"*, *supra* note 334, at 841 (explaining how unclear law enforcement rules can chill the behavior of police officers).

358. *See* Delaware v. Prouse, 440 U.S. 648, 653 (1979) ("The Fourth and Fourteenth Amendments are implicated in this case because stopping an automobile and detaining its occupants constitute a 'seizure' within the meaning of those Amendments, even though the purpose of the stop is limited and the resulting detention quite brief.").

359. *See* Whren v. United States, 517 U.S. 806, 810 (1996).

360. *See* Pennsylvania v. Mimms, 434 U.S. 106, 111 (1977).

361. *See* Michigan v. Long, 463 U.S. 1032, 1049 (1983).

362. *See* Texas v. Brown, 460 U.S. 730, 739-40 (1983) (plurality opinion).

363. *See* Carroll v. United States, 267 U.S. 132 (1925).

364. *See* United States v. Ross, 456 U.S. 798 (1982).

consent.[365] These rules are only the beginning; a significant body of law exists dealing with almost every aspect of traffic stops.

The key question for our purposes is this: what characteristics of traffic stops have allowed the courts to micromanage police procedures? I think there are two answers. First, the basic facts of traffic stops have proven stable across time, allowing courts to create rules based on reasonably ascertainable policy considerations. Courts have created traffic stop rules by balancing and weighing competing concerns such as privacy,[366] officer safety,[367] the need to preserve evidence,[368] and the administrability of various rules.[369] This enterprise is possible because from the time that the first Supreme Court traffic stop case was decided in the 1920s,[370] the basic operation and capacities of automobiles have remained more or less stable.[371] Policy concerns relating to the destruction of evidence have been based on a driver's ability to speed away in the vehicle and later dispose of the evidence, something that has not changed significantly over time.[372] Policy concerns relating to officer safety have focused on the risk that a suspect may have a handgun, a weapon that has remained essentially the same since the 1860s.[373] Although automobiles and handguns are themselves products of technology, they are stable products, changing little over many decades. As a result, a rule that makes sense today will likely make sense tomorrow.

The second factor allowing the courts to micromanage traffic stops is the familiarity of their facts. Judges understand traffic stops. They can picture what happened. They can strike the balance among privacy, safety, evidentiary integrity, and administrability because they

---

365. David A. Sklansky, *Traffic Stops, Minority Motorists, And The Future Of The Fourth Amendment*, 1997 SUP. CT. REV. 271, 275.

366. *See, e.g.*, Knowles v. Iowa, 525 U.S. 113, 116-17 (1998) (ruling that the search incident to arrest exception does not apply when a defendant is issued a citation but not arrested, because the defendant's privacy interest is not outweighed by concerns of officer safety or the need to preserve evidence for trial).

367. *See, e.g.*, Michigan v. Long, 463 U.S. 1032, 1049 (1983) (allowing protective sweeps of the areas of a car within the suspect's reach because "roadside encounters between police and suspects are especially hazardous, and that danger may arise from the possible presence of weapons in the area surrounding the suspect").

368. *Knowles*, 525 U.S. at 116.

369. *See* Atwater v. City of Lago Vista, 532 U.S. 318 (2001) ("Courts attempting to strike a reasonable Fourth Amendment balance [consider other factors along with] an essential interest in readily administrable rules." (citing New York v. Belton, 453 U.S. 454, 458 (1981))).

370. Carroll v. United States, 267 U.S. 132 (1925).

371. *See, e.g.*, LEON MANDEL, AMERICAN CARS 105-123 (1982) (describing the operation of a Ford Model T, the most popular car of the 1920s).

372. *Knowles*, 525 U.S. at 116.

373. *See generally* JOHN WALTER, HANDGUN: FROM MATCHLOCK TO LASER-SIGHTED WEAPON (1988) (discussing the evolution of handguns).

can appreciate the range of possible outcomes as well as the likelihood of those outcomes. Consider *Michigan v. Long*,[374] in which the Supreme Court announced that an officer with "specific and articulable" facts that support a reasonable belief that a driver or passenger may be dangerous can make a "protective sweep" of the areas of the vehicle within reach.[375] The Court created this rule after factoring in the relevant policy concerns, such as the facts that "roadside encounters between police and suspects are especially hazardous,"[376] "that danger may arise from the possible presence of weapons in the area surrounding a suspect,"[377] and the costs and benefits of a bright-line rule.[378] The Court's rule resulted from the Justices' assessment of competing policy concerns, which was in turn based on their understanding of the facts presented in traffic stop cases. Of course, we may not like a particular rule in a particular case; we may feel that a more or less privacy protecting rule would be better.[379] But the key is that judges are institutionally well-equipped to create such rules.[380] The combination of stable and readily understood facts enables judges to generate a reasonably coherent framework regulating police conduct at automobile traffic stops. Judges can create clear rules that strike a stable balance.

B. *The Fluctuating Relationship Between Surveillance and Privacy in Developing Technologies*

The picture changes considerably when we turn from cases with stable facts to situations involving technologies in rapid flux. Why? New technologies make what was hard easier, enabling us to achieve more, do more, or do so easier, faster, or more cheaply than before. Consider transportation.[381] Ten thousand years ago a person wishing to travel a long distance across land would likely walk; a thousand years ago she could ride a horse; a hundred years ago she could take a train;

---

374. 463 U.S. 1032 (1983).

375. *Id.* at 1048.

376. *Id.* at 1049.

377. *Id.*

378. *See id.* at 1049 n.14.

379. Commentators regularly condemn the Supreme Court's traffic stop cases for drawing lines in the wrong place, and in particular for giving too much weight to law enforcement concerns and too little weight to privacy interests. *See, e.g.*, David A. Moran, *The New Fourth Amendment Vehicle Doctrine: Stop and Search Any Car at Any Time*, 47 VILL. L. REV. 815 (2002); Steven A. Saltzburg, *The Supreme Court, Criminal Procedure and Judicial Integrity*, 40 AM. CRIM. L. REV. 133, 147-50 (2003).

380. 1 LAFAVE, ET AL., *supra* note 336, § 2.8 at 626-27.

381. *See generally* RUTH S. COWAN, A SOCIAL HISTORY OF AMERICAN TECHNOLOGY Ch. 5. (1997).

today, she can fly in an airplane. Each of these technological advances makes the travel faster and the journey easier. The new technologies make what was hard now easy — or at least easier — and in some cases make the once-impossible possible.[382]

In the context of the Fourth Amendment, technological change often upsets preexisting associations between law enforcement investigative steps and their privacy implications. Some new technologies make preexisting forms of surveillance more intrusive; others have the opposite effect.[383] The result is a complex and often-fluctuating relationship between surveillance and privacy. The stable relationship between law enforcement conduct and privacy in traditional cases is replaced by a fluid and often counter-intuitive relationship. As a result, the task of creating rules to protect privacy becomes significantly more dynamic and complex.

Consider the following example: A police officer stands on the public street outside a home and tries to peer inside, hoping to collect clues of criminal activity. How much can he learn about what is going on inside? The answer depends heavily on existing technologies. At a basic level, corrective eyeglasses may allow the officer to see through the windows of the home more clearly. Give the officer a flashlight, and he will be able to peer into the house through a window at night. Let the officer use an infrared imaging device, and he will be able to see a thermal image of the exterior of the home. Give him a shotgun microphone, and he may be able to hear communications inside.[384] All of these new technologies allow the officer to gather more evidence than before.

The dynamic works both ways, of course. People inside the home could take defensive measures against each of these technologies. For example, they could close the shutters or use tinted windows to block the flashlights and glasses. They could use thermal insulators to defeat the thermal imager. They could use soundproofing or white-noise generators to counter the shotgun microphone. All of these technologies block the surveillance. How much information can the police officer glean about the house from the public street? It depends on the technologies in use by both the police and the targets of the surveillance.

---

382. The effect is not always a change for the better, of course: technology enables new tools to be used for good or bad.

383. Most commentators focus on the first half of this equation while ignoring the second half, but both are equally important. Technologies can be used both to invade privacy and to block invasions of privacy. An obvious example of a technology that blocks invasions of privacy is encryption. *See generally* BRUCE SCHNEIER, SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD Pt. 2 (2000).

384. *See* Mark G. Young, Note, *What Big Eyes And Ears You Have!: A New Regime For Covert Governmental Surveillance*, 70 FORDHAM L. REV. 1017, 1031 (2001) (describing shotgun microphones).

Wiretapping provides another example. Consider the question, how invasive is wiretapping? In *Berger v. New York*,[385] Justice Douglas called wiretapping "a dragnet" that "intercepts the most intimate of conversations."[386] But whether that is true depends on the type and form of information that travels across the wires to be tapped. This is not constant: as technology develops, the type of information can change. The invasiveness of wiretapping fluctuates with time. When the Supreme Court decided *Berger* in 1967, telecommunications wires primarily carried telephone signals. Tapping a wire was a gross invasion of privacy: it meant listening in on a private telephone conversation.[387] Today that is less likely to be true. For example, many wires carry Internet communications, which may include many types of much less private communications. Some Internet communications are as private as telephone calls, but many are not:

> If you were to select a random spot on the Internet and watch the Internet traffic streaming by, you would pick up e-mails, Web pages in transit, commands sent to remote servers, picture or music files, network support traffic, and almost everything else in cyberspace. Many of these communications would deserve privacy, but others would not.[388]

Fast forward to the future. Technologists predict that in a decade or two, Internet communications routinely will be encrypted — scrambled using mathematical algorithms — using a form of essentially unbreakable encryption.[389] When Internet users encrypt their communications, wiretapping will become largely ineffective. The police can tap the line, but obtain only a meaningless string of 0s and 1s that can prove difficult if not impossible to descramble. If this proves to be the case, wiretapping will on average be much less invasive than it was in the 1960s. And if it happens it will really be a return to the past: encrypting communications was a common measure in the telegraph era of the 1860s, before the telephone was even invented.[390] In those days, tapping a wire was only one step of several needed to eavesdrop on a private communication.[391]

The social importance of technologies can also change as related technologies develop. The public telephone provides an interesting

---

385. 388 U.S. 41 (1967).

386. *Id.* at 65 (Douglas, J., concurring).

387. *See id.*

388. Orin S. Kerr, Essay, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 WASH. & LEE. L. REV. 1287, 1300 (2000).

389. *See, e.g.*, LESSIG, *supra* note 10, at 35-39 ("Cryptography will change everything . . . ."); SCHNEIER, *supra* note 383, at 85-100.

390. *See, e.g.*, SIMON SINGH, THE CODE BOOK 60-79 (1999) (discussing the widespread use of encryption in the context of telegraph communications).

391. *See id.* at 75.

example. In the 1960s, public telephones provided a vital means of communication for many Americans. *Katz v. United States*[392] gave this role constitutional significance: in support of the Court's conclusion that the Fourth Amendment protected Charles Katz while he used the pay phone booth, the Court added a single line of explanation: "To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[393] Perhaps the Court did not mean this literally; perhaps it is rhetorical fluff. But if taken at face value, it would create a serious question as to the continuing vitality of *Katz*. The reason is that public telephones no longer play a vital role in private communication. The pay telephone has been largely eclipsed by the cell phone. Since the mid-1990s, over 100 million Americans have purchased cell phones, and the number of public telephones in the United States has dropped by more than 30%.[394] Existing pay phones are used about half as much today as they were in 1996.[395] As a *Chicago Tribune* headline recently announced, "Pay Phones May Go the Way of Dinosaurs."[396] The Supreme Court could reasonably declare the public telephone "vital" in 1967; today it could not.

These examples highlight how technological change complicates the creation of Fourth Amendment-like rules. The privacy implications of a rule at one time may be quite different from the implications of the rule at another time. The rules are based on often-unstable assumptions, and the law's challenge is to respond to the changing facts. The question is, which branch of government is best equipped to respond to these difficulties? Legislatures or courts?

C. *The Challenge of Ex Post Decisionmaking*

Courts and legislatures generate rules of criminal procedure in somewhat different ways, subject to different constraints. A full recounting of the differences is beyond the scope of this paper. But I will sketch the three basic differences critical to a comparison of the institutional competence of courts and legislatures in this context: ex ante versus ex post decisionmaking, flexibility, and the information environment of judicial versus legislative rules.

---

392. 389 U.S. 347 (1967).

393. *Id.* at 352.

394. *See* Yuki Noguchi, *Requiem for the Pay Phone: As Cell Phone Use Increases, an Icon Gradually Dies*, WASH. POST, Dec. 30, 2002, at E1.

395. *See* Virgil Larson, *Cutting the Cord on Pay Phones*, OMAHA WORLD-HERALD, Dec. 28, 2002, at 1d.

396. John Van, *Pay Phones May Go the Way of Dinosaurs*, CHI. TRIB., June 13, 2002, at 1.

The first difference is that legislatures typically create generally applicable rules ex ante,[397] while courts tend to create rules ex post in a case-by-case fashion.[398] That is, legislatures enact generalized rules for the future, whereas courts resolve disputes settling the rights of parties arising from a past event.[399] The difference leads to Fourth Amendment rules that tend to lag behind parallel statutory rules and current technologies by at least a decade, resulting in unsettled and then outdated rules that often make little sense given current technological facts.

Consider the hurdles that must be overcome before the courts resolve how the Fourth Amendment applies to a new technology. Because the Fourth Amendment applies only to actual searches, not to technologies that merely have the potential to conduct searches,[400] courts generally cannot pass on how the Fourth Amendment applies to a technology until long after a technology has been introduced. For a trial court to address the Fourth Amendment implications of a technology, the technology must be used by the government in the course of investigating a criminal offense; the use of the technology must yield evidence of a crime; it must lead to an arrest; and then it must lead to a constitutional challenge requiring judicial resolution.[401] Appellate decisions come only much later. Because plea agreements usually require a defendant who pleads guilty to waive a right of appeal, and the overwhelming majority of cases end in a plea,[402] appellate decisions come only in the rare case in which a defendant has been convicted at trial and then appeals, or else signs a conditional plea allowing an appeal. When an appeal is heard, it is usually decided more than a year after the initial trial court's decision. Very few appeals lead to published, precedential opinions. Even if the issue does lead to a published decision of an appellate court, Supreme Court review is not likely; the Court hears only about 80 or 90 cases a year. If

---

397. *See* Henry M. Hart, Jr., *The Aims of the Criminal Law*, LAW & CONTEMP. PROBS. Summer 1958, at 401, 412.

398. *See id.* at 429-30, 435.

399. *See id.* at 412 ("A legislature deals with crimes always in advance of their commission . . . . It deals with them always by directions formulated in *general terms*.").

400. United States v. Karo, 468 U.S. 705, 712 (1984) (noting that the court has never held that "potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment").

401. I am assuming here that the court would address the Fourth Amendment issues in the context of a motion to suppress. An alternative route would be a civil action brought under *Bivens* or 42 U.S.C. § 1983, which would generally require notice of the use of the technology and measurable damages.

402. *See* U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE STATISTICS, SOURCEBOOK OF CRIMINAL JUSTICE STATISTICS 432 (1999) (indicating that 1.4% of federal felony defendants were acquitted after trial, 4.3% were convicted after trial, the cases of 10.4% were dismissed, and 83.9% pleaded guilty or nolo contendere).

the Supreme Court does agree to resolve the case eventually, it is likely to happen several years after the circuit courts have first addressed the issue.[403]

The history of Fourth Amendment law reflects this gap. The Supreme Court first considered the Fourth Amendment implications of wiretaps almost six decades after the invention of the telephone.[404] Pen registers were in widespread use by the 1960s,[405] but the Supreme Court did not pass on whether their use violated the Fourth Amendment until 1979.[406] Even today, no Article III court at any level has decided whether an Internet user has a reasonable expectation of privacy in their e-mails stored with an Internet service provider;[407] whether encryption creates a reasonable expectation of privacy;[408] or what the Fourth Amendment implications of the "Carnivore" Internet surveillance tool might be.[409] The technologies exist, and in the case of encryption and e-mail, are used by millions of Americans everyday. But no one really knows how the Fourth Amendment applies to them.

This delay carries important consequences for the clarity of judicial rulemaking. Years may pass before a court considers how the Fourth Amendment regulates use of a new technology; many more years may pass before the issue is resolved definitively. By the time the courts decide how a technology should be regulated, however, the factual record of the case may be outdated, reflecting older technology rather than more recent developments.[410] Further, once the law appears to be settled, the rapid pace of technological change may make it difficult to know how *future* courts might resolve the same problem. Existing precedents may have little force: an appellate decision based on a factual record created a few years before may no longer apply just a

---

403. *See* H.W. PERRY, JR., DECIDING TO DECIDE: AGENDA SETTING IN THE UNITED STATES SUPREME COURT 230-34 (1991) (explaining that the Court often allows issues to percolate through the lower courts before the Court will resolve it).

404. The telephone was invented in 1876. *Olmstead* was decided in 1928. *See supra* note 246 and accompanying text.

405. *See* United States v. Guglielmo, 245 F. Supp. 534 (N.D. Ill. 1965) (considering the legality of a pen register device).

406. *See* Smith v. Maryland, 442 U.S. 735 (1979).

407. *See* United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002) (noting in dicta that "[w]hile it is clear . . . that Congress intended to create a statutory expectation of privacy in e-mail files, it is less clear that an analogous expectation of privacy derives from the Constitution").

408. *See* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy"?*, 33 CONN. L. REV. 503, 513 (2001) ("The courts have not yet faced a direct Fourth Amendment challenge to the decryption of encrypted Internet communications.").

409. *See generally* Frank J. Eichenlaub, Comment, *Carnivore: Taking A Bite Out Of The Fourth Amendment?*, 80 N.C. L. REV. 315 (2001).

410. *See* Stuart Minor Benjamin, *Stepping Into the Same River Twice: Rapidly Changing Facts and the Appellate Process*, 78 TEX. L. REV. 269 (1999).

few years later. As Stuart Benjamin has noted, "[r]apidly changing facts weaken the force of stare decisis by undermining the stability of precedents. Appellate opinions are only as robust as the facts on which they are based. When those facts evaporate, the opinion on which they rest is weakened as well."[411] Consider the lower court's findings about the Internet in the litigation that led to the Supreme Court's decision in *Reno v. ACLU*.[412] The facts were accurate for 1996, but are not necessarily accurate today.[413] Because constitutional rules may be based on changing technological facts, it may be difficult know whether a Fourth Amendment rule that is valid one day is valid the next.[414]

Legislative rules are different. Legislatures can act at any time, even when a technology is new. As a practical matter, legislatures often will wait for public concern to surface before regulating a new technology. But recent history suggests that legislatures usually act at a surprisingly early stage, and certainly long before the courts. For example, while the courts have not yet decided how the Fourth Amendment protects stored e-mails, Congress enacted a comprehensive regime to protect the privacy of e-mails *in 1986* in the form of the Electronic Communications Privacy Act.[415] Congress regulated the privacy of e-mail before most Americans had even heard of e-mail. Similarly, Congress enacted laws to regulate the "Carnivore" Internet surveillance system in 2001 before any Fourth Amendment challenges were raised to its use.[416]

Congress has even acted before a technology was invented. For example, Congress recently passed a law blocking the Pentagon's proposed "Total Information Awareness" (TIA) program, which would have funded research into the development of computer data-mining technology.[417] Unburdened by the procedural barriers that limit and delay judicial power, legislatures can enact comprehensive rules far ahead of current practice rather than decades behind it.

---

411. *Id.* at 272.

412. 521 U.S. 844 (1997).

413. *See* LESSIG, *supra* note 10, at 216; Benjamin *supra* note 410, at 294.

414. *Cf.* Ashcroft v. ACLU 124 S.Ct. 2783, 2794 (2004) (noting that after a delay of five years, "the factual record [in an Internet-related case] does not reflect current technological reality.").

415. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended as a note to 18 U.S.C. § 2510 (2000)).

416. *See* Kerr, *Internet Surveillance Law After the USA Patriot Act*, *supra* note 323, at 648-58 (discussing provisions of the USA Patriot Act designed to regulate the Internet surveillance tool known as Carnivore).

417. Audrey Hudson, *'Supersnoop' Scheme Blocked Pending Review by Congress; Privacy Issues Cited in Pentagon TIA Project*, WASH. TIMES, Feb. 13, 2003, at A1. ("Key lawmakers have agreed to block funding for the Pentagon's Total Information Awareness project until Congress can review the technology's effect on privacy and civil liberties.").

D. *The Need for Flexibility in Light of Changing Facts*

A second difference between judicial and legislative rulemaking concerns their operative constraints. Judicial rulemaking is limited by strong stare decisis norms that limit the ability of judicial rules to change quickly; in contrast, legislatures enjoy wide-ranging discretion to enact new rules. The difference favors legislatures when technology is in flux because the privacy implications of particular rules can fluctuate as technology advances. To ensure that the law maintains its intended balance, it needs mechanisms that can adapt to technological change. Legislatures are up to the task; courts generally are not. Legislatures can experiment with different rules and make frequent amendments;[418] they can place restrictions on both public and private actors; and they can even "sunset" rules so that they apply only for a particular period of time. The courts cannot.[419] As a result, Fourth Amendment rules will tend to lack the flexibility that a regulatory response to new technologies may require.

The statutory framework that governs Internet privacy demonstrates the flexibility and creative potential of legislative approaches. Congress enacted the Electronic Communications Privacy Act ("ECPA") in 1986 to regulate the privacy of Internet communications.[420] Since that time, Congress has amended the framework no less than eleven times: once in 1988,[421] twice in 1994,[422] three times in 1996,[423] once 1998,[424] twice in 2001,[425] and twice in 2002.[426] Some of those changes were only minor technical amendments, while others were more significant alterations to the statutory scheme. Moreover, the structure of Congress's statutory Internet privacy laws demonstrates how legislative rules can impose

---

418. *See* DONALD L. HOROWITZ, THE COURTS AND SOCIAL POLICY 35 (1977).

419. *See id.* at 36-37.

420. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as a note to 18 U.S.C. § 2510).

421. *See* Anti-Drug Abuse Act of 1988, Pub. L. 100-690, 102 Stat. 4398.

422. *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994); Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 330003(b), 108 Stat. 1796.

423. *See* Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214; Intelligence Authorization Act for Fiscal Year 1997, Pub. L. No. 104-293, 110 Stat. 3461 (1996); Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488.

424. *See* Telemarketing Fraud Prevention Act of 1998, Pub. L. No. 105-184, 112 Stat. 520.

425. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272; Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, 115 Stat. 1394 (2001).

426. *See* 21st Century Department of Justice Appropriations Act, Pub. L. No. 107-273, 116 Stat. 1758 (2002); Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135.

creative and flexible regulatory regimes involving new technologies. For example, Congress opted to regulate both public and private parties to best protect privacy. This would be difficult if not impossible under the Fourth Amendment, which regulates only the government and private parties acting on the government's behalf.[427] But ECPA recognizes that private parties acting on their own can pose a serious threat to Internet privacy: if America Online can look through the e-mails of its 30 million subscribers and disclose the evidence to the police without restriction, this would gut Internet privacy protections. The Fourth Amendment does not restrict this disclosure, but ECPA does:[428] in addition to restricting the ability of law enforcement to order private ISPs to disclose communications to law enforcement,[429] the law also restricts the ability of private ISPs to disclose communications to law enforcement voluntarily.[430]

Congress has also created new court orders as needed to deal with novel Internet privacy problems. Under the 1986 Act, for example, the government needed a search warrant to compel ISPs to disclose certain information, but could obtain the rest with a mere subpoena.[431] Convinced that some of the information ISPs collected deserved more privacy protection, Congress invented a new court order in 1994, a "specific and articulable facts" court order.[432] The new order has a threshold about midway between that for a subpoena and a search warrant:[433] to collect the information, the government must apply to a court and offer "specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation."[434] This new court order is only one of many Congress has created: a recent tally counts at least eight statutory thresholds that Congress has used in the area of Internet surveillance law alone.[435]

---

427. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("[The Fourth Amendment] is 'wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any government official.' " (quoting Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting))).

428. *See* S. REP. NO. 99-541, at 36 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3590.

429. *See* 18 U.S.C. § 2703 (2000).

430. *See* 18 U.S.C. § 2702 (2000).

431. *See* H.R. REP. NO. 103-827, at 12 (1994), *reprinted in* 1994 U.S.C.A.A.N. 3489, 3492.

432. 18 U.S.C. § 2703(d) (2000). The need for this special court order was urged by Senator Leahy. *See* H.R. REP. NO. 103-827, at 12 (1994), *reprinted in* 1994 U.S.C.A.A.N. 3489, 3492.

433. *See* United States v. Kennedy, 81 F. Supp. 2d 1103, 1109 n.8. (D. Kan. 2000) (citing H.R. REP. NO. 103-827, at 31-32 (1994), *reprinted in* 1994 U.S.C.A.A.N. 3489, 3511-12).

434. *Id.*

435. *See* Kerr, *Internet Surveillance Law After the USA Patriot Act*, *supra* note 323, at 620-21 (explaining different statutory thresholds currently used by Congress to regulate Internet surveillance law).

Congress has also experimented with rules through a "sunset" mechanism.[436] When Congress passed the USA Patriot Act in October 2001, it granted many powers to the government for just four years: the extra powers "sunset" on December 31, 2005, when the law will revert back to its pre-Patriot Act state.[437]

It is far harder for the courts to adopt such flexible rules under the Fourth Amendment.[438] Putting aside the merits of such an approach from the standpoint of normative constitutional theory, the task would create enormous practical headaches. To allow the governing rules to change as needed over time, courts would be forced either to expressly change the governing rules at regular intervals or else articulate the governing rule using a standard that keeps the result unclear to incorporate changed circumstances. Stare decisis norms make the first option unrealistic; it's hard to imagine the courts creating new rules every few years to keep the law up to date. But the latter option leads to intolerable uncertainty. The result is constitutional law's version of the Heisenberg uncertainty principle in quantum physics;[439] you can know the law at one time or you can know its general direction, but you can't know both at the same time.

We can see the challenge of changing facts in Justice Scalia's effort to craft a rule for sense-enhancing devices in *Kyllo v. United States*.[440] Justice Scalia recognized the key difficulty: thanks to technological change, use of a particular sense-enhancing device might seem objectionable in one era but routine in another.[441] He thus tried to craft a rule that would apply across time, producing different results at different times. Recall the Court's holding in that case: "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[442] Notably, this

436. *See id.* at 607.

437. *See id.*

438. *See* HOROWITZ, *supra* note 418, at 36.

439. The Heisenberg uncertainty principle is an observation of quantum physics that the more precisely the position of a particle is determined, the less precisely the momentum of that particle can be known. *See* WERNER HEISENBERG, PHYSICS AND PHILOSOPHY: THE REVOLUTION IN MODERN SCIENCE 47-48 (1958); *see also* Laurence H. Tribe, *The Curvature of Constitutional Space: What Lawyers Can Learn From Modern Physics*, 103 HARV. L. REV. 1, 17 (1989).

440. 533 U.S. 27 (2001).

441. During the oral argument of an earlier case involving the Internet, Justice Scalia commented, "This is an area where change is enormously rapid. Is it possible that this statute is unconstitutional today, or was unconstitutional 2 years ago when it was examined on the basis of a record done about 2 years ago, but will be constitutional next week?" Transcript of Oral Argument at *49, Reno v. ACLU, 521 U.S. 844 (1997) (Reno II) (No. 96-511), *available at* 1997 WL 136253.

442. *Kyllo*, 533 U.S. at 40.

rule does not mean that the warrantless use of devices such as thermal imagers directed at the home necessarily violates the Fourth Amendment; rather, the devices will violate the Fourth Amendment *until they enter "general public use."* At some point in the future, thermal imaging devices will likely come into widespread use: they are increasingly used as non-contact thermometers by hobbyists, electricians, and mechanics, and can be purchased on-line for $40.[443] But how can anyone determine when the use of a thermal imaging device is in "general public use" so that the government can use one without a warrant?

An example illustrates the difficulty. Imagine that in 2010, 5% of the population owns some kind of thermal imaging device, and a police officer decides to use one in the same way that the police did in the *Kyllo* case. The police officer uses the device, which leads to a warrant and an arrest in 2011. In 2012, the defendant challenges the procedure before the trial court. The trial court concludes that 5% of the population owned thermal imaging devices in 2010, but also recognizes that 8% own such devices by the time of the hearing in 2012. The defendant is convicted and the defendant appeals: the briefing occurs in 2013, the oral argument is held in early 2014, and the appellate court issues its decision in late 2014. Assume that by late 2014, 15% of the public owns thermal imaging devices. What is the relevant date that the appellate court should use to determine whether thermal imaging devices are in "general public use"? The time of the search? The trial court hearing? The filing of the appellate briefs? Oral argument? The appellate court's decision?[444] Under the *Kyllo* test, the use of the imaging device may be unconstitutional early in the case but constitutional by the later stages. And what if thermal imaging devices come into widespread use in one generation, but later become obsolete thanks to a subsequent technology, and fall out of "general public use"? Does that mean that their use will be unconstitutional again?

One might say that these questions are simply the kind of line-drawing inquiries that lawyers can raise about the uncertainties of any new rule. But I disagree. The *Kyllo* rule is unusually unclear; it leaves the government with little guidance about what they can do and when

443. Thermal imagers can be used to check for heat leaks in a home, test packages for broken seals, and test automotive or household electrical systems for poor contacts and short circuits. *See* InfraredThermography.com, http://www.infraredthermography.com/applicat.htm (last visited June 3, 2004); Thermal Imaging, Some Uses, http://www.spectra-uk.com/thermuse.htm (last visited June 4, 2004); Uses of Thermal Imaging, http://www.thermis.force9.co.uk/uses_.html (last visited June 4, 2004). I recently purchased my own infrared thermal imaging device for $39.95 from www.pythons.com, a website devoted to reptile breeding. But this is a subject for another article.

444. *See* Benjamin, *supra* note 410, at 312-68(noting the various options a court faces when facts change in the course of litigation).

they can do it. These uncertainties follow from the need to create a single rule that applies ex post in different ways as technology changes. Because the ideal rule may change as the technology advances, *Kyllo* keeps outcomes uncertain to make sure that the outcome can change as the technological facts change. The resulting rule inevitably sacrifices certainty ex ante to allow the courts to pronounce outcomes ex post.

E. *The Judicial Information Deficit*

The third important difference between judicial rules and legislative rules relates to the information environment in which rules are generated. Legislative rules tend to be the product of a wide range of inputs, ranging from legislative hearings and poll results to interest group advocacy and backroom compromises. Judicial rules tend to follow from a more formal and predictable presentation of written briefs and oral arguments by two parties.[445] Once again, the difference offers significant advantages to legislative rulemaking. The task of generating balanced and nuanced rules requires a comprehensive understanding of technological facts. Legislatures are well-equipped to develop such understandings; courts generally are not.

The information environment of judicial rulemaking is usually poor.[446] Judges decide cases based primarily on a brief factual record, narrowly argued legal briefs, and a short oral argument.[447] They must decide their cases in a timely fashion, and can put only so much effort into any one case.[448] In some contexts, these limitations do not impose a heavy burden on effective judicial rulemaking. Recall the automobile traffic stop cases. Because judges can readily understand traffic stops, a brief record and narrow argument is generally sufficient to allow judges to create rules governing the specific facts at hand. In contrast, cases involving new technologies such as wireless networks, public-key encryption, and data-mining technologies raise more complicated issues. Judges struggle to understand even the basic facts of such technologies, and often must rely on the crutch of questionable

445. *See, e.g.*, Lon. L. Fuller, *The Forms and Limits of Adjudication*, 92 HARV. L. REV. 353, 363-87 (1978). This description of the judicial process may be less true in the context of modern civil litigation, *see, e.g.*, Owen M. Fiss, *The Supreme Court, 1978 Term — Foreword: The Forms of Justice*, 93 HARV. L. REV. 1, 39-44 (1979), but is still quite accurate in the context of criminal litigation.

446. *See* HOROWITZ, *supra* note 418, at 45-51 (noting the difficulty courts have in ascertaining "social facts," defined as "recurrent patterns of behavior on which policy must be based").

447. On occasion, an *amicus curiae* brief may also shed light on technological practice.

448. *See* Henry M. Hart, Jr., *Foreword: The Time Chart of the Justices*, 73 HARV. L. REV. 84, 99-100 (1959) (stressing the limited time that the Supreme Court can devote to any particular case, and arguing that the Court should take fewer cases to provide each case with "fresh illumination of personal research and of hard, independent thought").

metaphors to aid their comprehension.[449] Judges generally will not know whether those metaphors are accurate, or whether the facts before them are typical or atypical given the technology of the past or the present. These dynamics make it easy for judges to misunderstand the context of their decisions and their likely effect when technology is in flux. Judges who attempt to use the Fourth Amendment to craft broad regulatory rules covering new technologies run an unusually high risk of crafting rules based on incorrect assumptions of context and technological practice.[450] The context of judicial rulemaking is unusually conducive to high rates of error when technology is in flux.

The recent work of Cass Sunstein and Adrian Vermeule has made important contributions to this point. In their recent article *Interpretations and Institutions*,[451] Sunstein and Vermeule consider how the institutional capacities of various rulemakers should inform their interpretive exercises. Their critique of Professor Lessig's theory of constitutional translation is particularly relevant here.[452] Lessig's theory of translation requires judges to update constitutional rules as facts change, such that the overall effect of the rule given the new facts will echo the original effect of the rule given the original facts.[453] Applying this approach, Lessig supports a broad reading of the Fourth Amendment in new technologies, as I noted at the beginning of this section.[454] Sunstein and Vermeule challenge the feasibility of this approach, arguing that judges often will lack the institutional capacity to "update" constitutional rules effectively as facts change:

> It takes great confidence in [judicial] capacities to think that judges can identify the net effects of [factual change] with enough precision to warrant jettisoning clear constitutional provisions and settled constitutional rules. . . . There is little reason to believe that generalist judges, devoting a brief time to the subject and possessed of limited

449. *See* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 359-62 (2003) (explaining how courts applying law to the Internet can choose between virtual and physical metaphors, but there is little to guide the choice of metaphor).

450. *See* Cass R. Sunstein, *Foreword: Leaving Things Undecided*, 110 HARV. L. REV. 6, 18 (1996) ("Lack of information is thus a crucial argument for decisional minimalism."); Sunstein, *supra* note 345, at 363 ("On the underlying facts, things are changing very rapidly, and courts know relatively little; but the facts are crucial to the analysis."). *Cf.* Edward Lee, *Rules and Standards for Cyberspace*, 77 NOTRE DAME L. REV. 1275, 1356 (2002). ("We should not encourage judicial activism in cyberspace cases if the courts lack sufficient expertise and information to address the rapidly changing circumstances.").

451. Cass R. Sunstein & Adrian Vermeule, *Interpretations and Institutions*, 101 MICH. L. REV. 885 (2003).

452. *See id.* at 941-44.

453. *See* Lawrence Lessig, *Fidelity in Translation*, 71 TEXAS L. REV. 1165 (1993).

454. *See* LESSIG, *supra* note 10, at 111-21.

> information, can form even a plausible view of the relevant complexities.[455]

Justice Stephen Breyer has also recognized the difficulties of judicial creation of privacy rules in new technologies in his recent extra-judicial writing.[456] The problem of privacy in new technologies "is unusually complex,"[457] Justice Breyer noted, involving changing public perceptions, changing laws, and changing technologies. "These circumstances mean that efforts to revise privacy law to take account of the new technology will involve . . . the balancing of values in light of predictions about the technological future."[458] Courts should not preempt this process through broad constitutional rulemaking, Breyer reasoned. While courts have a role to play, that role should be modest, allowing the "participatory democratic process"[459] to work through issues first. This approach echoes the caution of Justice Breyer's opinion in a First Amendment case, *Denver Area Educational Telecommunications Consortium, Inc. v. FCC*.[460] Justice Breyer voted to uphold rules permitting cable system operators to prohibit "patently offensive" indecent programming transmitted over leased access channels.[461] Although the parties framed the issue as a choice of how to analogize cable systems, Justice Breyer upheld the statute on a narrower ground that avoided reliance on a definitive analogy:

> no definitive choice among competing analogies (broadcast, common carrier, bookstore) allows us to declare a rigid single standard, good for now and for all future media and purposes. . . . Rather, aware as we are of the changes taking place in the law, the technology, and the industrial structure related to telecommunications . . . we believe it unwise and unnecessary definitively to pick one analogy or one specific set of words now.[462]

By declining to resolve definitively how the First Amendment applies to cable systems, Justice Breyer avoided committing to an answer that might seem appropriate today but cause problems as technology and social practices evolve.

The limitations of judicial rulemaking in the Fourth Amendment context are illustrated by two recent cases applying the Fourth Amendment to computers. Let's start with *United States v. Bach*.[463]

---

455. Sunstein & Vermeule, *supra* note 451, at 943.

456. *See* Stephen Breyer, *Our Democratic Constitution*, 77 N.Y.U. L. REV. 245 (2002).

457. *Id.* at 261.

458. *Id.* at 262.

459. *Id.* at 263.

460. 518 U.S. 727 (1996).

461. *See id. passim* (plurality opinion).

462. *Id.* at 741-42.

463. No. CRIM.01-221, 2001 WL 1690055 (D. Minn. Dec. 14, 2001), *rev'd* 310 F.3d 1063 (8th Cir. 2002).

Bach raised a constitutional challenge to the law enforcement practice of faxing search warrants to ISPs for information on their servers.[464] Rather than execute the search at the ISP, the police in *Bach* ordered the ISP that possessed the information to collect the evidence on its own and send it to law enforcement.[465] The defendant argued that the Fourth Amendment required law enforcement to be physically present at the ISP (in this case, the California-based ISP Yahoo!) to execute the warrant or at least to oversee the process. According to the defendant, merely faxing the warrant to Yahoo! threatened privacy because it granted too much discretion to Yahoo! employees who could easily exceed the scope of the warrant.[466] The district court agreed, ruling that the Fourth Amendment required a law enforcement presence at the ISP to protect privacy:

> Police officers have taken an oath to uphold federal and state Constitutions and are trained to conduct a search lawfully and in accordance with the provisions of a warrant. Civilians, on the other hand, are not subject to any sort of discipline for failure to adhere to the law. In fact, an internet service provider is immune from suit so long as it is providing assistance in accordance with the terms of a warrant. Without an officer present, this conditional grant of immunity may become an irrefutable protection for internet service providers to conduct searches that traverse the clearly defined limits of a warrant. In the particular context of this case, there were no safeguards ensuring that the Yahoo employees conducting the search and seizure of information in [the defendant]'s e-mail account were cautiously abiding by the terms of the . . . warrant. Accordingly, the execution of the . . . warrant does not pass constitutional muster.[467]

This reasoning reflected the court's best guess as to how ISPs comply with court orders to produce records, which informed the court's sense of what method for executing the warrant best protected privacy. The district court judge apparently assumed that the skills required to search a computer server are similar to the skills required to search physical property. In a search of physical property, an untrained person would be likely to destroy more property and invade more privacy than a trained officer. Applying this rationale to a search of a computer, the court reasoned that an officer's physical presence was required to protect privacy and comply with the Fourth Amendment.

---

464. *See* UNITED STATES DEPARTMENT OF JUSTICE, *supra* note 331, at 98 ("Once a magistrate judge signs the warrant . . . investigators ordinarily do not themselves search through the provider's computers in search of the materials described in the warrant. Instead, investigators serve the warrant on the provider as they would a subpoena, and the provider produces the material described in the warrant.").

465. *See Bach*, 2001 WL 1690055, at *1.

466. *See id.* at *2.

467. *Id.* at *3 (citations omitted).

The district court's guess was wrong, however, at least based on current technology. On appeal, Yahoo! and a consortium of other ISPs filed an amicus brief explaining how ISPs comply with search warrants for data stored on computer servers.[468] The brief explained that searches for information stored in an ISP's computers require technical expertise and specialized knowledge to extract the information from the ISP's network.[469] Because of these technical details, the brief explained, police officers are

> in no position to supervise or instruct the service provider's technicians as they search for the information requested in the warrant; [the technicians] must conduct the search themselves, from their computer terminals. The police officer waiting in the lobby while the technician works away on the computer does not in any way safeguard anyone's Fourth Amendment rights.[470]

The Eighth Circuit reversed the district court, relying largely on the reasoning of the Yahoo! brief.[471] This time, the court held that the practice of faxing warrants was constitutionally reasonable. The court relied heavily on practical reasons, including that "the actual physical presence of an officer would not have aided the search (in fact may have hindered it),"[472] and that "the technical expertise of Yahoo!'s technicians far outweighs that of the officers."[473] How did the Eighth Circuit judges know these facts? Because they read them in Yahoo!'s amicus brief.

While the Court of Appeals corrected the district court's error in *Bach*, the error illustrates the difficulty courts encounter trying to regulate new technologies through the Fourth Amendment. The district court guessed about ISP practices, and based a constitutional rule on that guess. But the guess turned out to be incorrect. Fortunately, the district court's ruling led to an amicus brief on appeal that corrected the misunderstanding. But this will happen only rarely; in most cases, courts will not possess an informed understanding of the technical facts they need to appreciate the technology they are attempting to regulate. They will simply guess, and create rules that may or may not do what the courts think they will do. Because the courts tend to lack knowledge of the broader technological context, they struggle to create workable and sensible rules governing that technology.

---

468. Brief of *Amici Curiae* Yahoo!, Inc., et al., *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238) (on file with author).

469. *See id.* at 6-7.

470. *Id.* at 7.

471. United States v. Bach, 310 F.3d 1063 (8th Cir. 2002).

472. *Id.* at 1067.

473. *Id.*

Trulock v. Freeh[474] provides another interesting example. Notra Trulock was a Department of Energy official investigated by the FBI for allegedly disclosing classified information.[475] In the course of the investigation, the FBI obtained the consent of Trulock's girlfriend to search a computer that they both used. Trulock later filed a *Bivens* action against the FBI, alleging that the FBI "searched" Trulock's password-protected files stored in the computer in violation of the Fourth Amendment.[476] The complaint alleged that the girlfriend's consent to search the computer did not allow the FBI to search the password-protected files. The Fourth Circuit agreed, holding that searching the password-protected files was like opening a locked box belonging to Trulock.[477] The panel split only on whether the Fourth Amendment violation was sufficiently clear that qualified immunity allowed civil liability for the violation: two judges said no, one said yes.[478] But all three judges agreed that the search violated the Fourth Amendment.

But no one asked the more basic question: What exactly did it mean to "search" a password-protected file? In other words, what was it that violated the Fourth Amendment? The opinions suggest that the judges understood "searching" the password-protected file to be something akin to rummaging through a locked box.[479] But this metaphorical understanding tells us very little; Trulock's allegation that the FBI had "searched" the password-protected files could mean several different things. Perhaps the password-protected files were encrypted, and the agents merely saw the ciphertext, not the

---

474. 275 F.3d 391 (4th Cir. 2001). In the interests of full disclosure, I should acknowledge that I was a lawyer at the Justice Department at the time the *Trulock* case was briefed, and served as an informal adviser on the briefing of the case.

475. *See id.* at 397-98.

476. *Id.* at 399.

477. *Id.* at 403 ("Although Conrad had authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files. . . . Trulock's password-protected files are analogous to the locked footlocker inside the bedroom.").

478. Judge Gregory and District Judge Legg said "no", *see id* at 403; Judge Michael authored a separate opinion saying "yes":

> I respectfully disagree . . . with the majority's view that the defendants are entitled to qualified immunity because there was no clearly established law saying that one co-user's consent to search a computer does not extend to the password-protected files of another co-user when the consenting co-user does not know the other's passwords. I would reject the defendants' qualified immunity defense because the unlawfulness of searching Trulock's password-protected files was readily apparent . . . .

Id. at 407 (Michael, J., concurring in part and dissenting in part).

479. *See id.* at 403 (analogizing the case to *United States v. Block*, 590 F.2d 535, 540-42 (4th Cir. 1978), which had held that a mother's consent to a search of her son's bedroom did not allow a search of a locked footlocker in the room, and stating that "Trulock's password-protected files are analogous to the locked footlocker inside the bedroom."); *id.* at 406-07 (Michael, J., concurring in part and dissenting in part).

understandable plaintext. Or maybe the agents performed string queries for keywords that appeared in Trulock's files. Or maybe the agents guessed Trulock's password and then viewed his private files. The opinion doesn't say what exactly occurred. The *Trulock* court neither explained what kind of password protection Trulock used, nor what the agents might have done to circumvent the password protection and "search" the files.

The difference is important, however, because many different types of password protection exist, all of which can be circumvented in various ways.[480] Without knowing the technical details of what happened in Trulock, it's hard to know with any precision what the *Trulock* opinion prohibits. In other words, the more you understand about password-protection, the less clear the court's rule becomes. How did this happen? The likely explanation is that the judges in *Trulock* simply didn't understand enough about the technology of password-protection to know that their opinion left the rule unclear. The judges analogized searching the password-protected computer files to searching through a locked box, but their failure to appreciate the technology left the meaning of the decision a mystery.

To be sure, legislative rulemaking is not a panacea. At the same time, the information environment of legislative rulemaking is superior to that of judicial rulemaking in the context of developing technologies. Legislatures can receive input from a wide range of sources, and can use these inputs to generate well-informed rules. The open legislative process and the accompanying public scrutiny tend to ferret out rules that are particularly unbalanced, and often lead to amendments that temper proposed rules that go too far in either direction. For example, Congress generally legislates in the area of high-tech privacy only after holding extensive hearings in which experts testify and comment on various technologies and regulatory strategies.[481] Legislators typically ask both the Justice Department and civil liberties groups for comment, and consider objections from both sources before voting on legislation. The legislature can also amend

---

480. *See* SCHNEIER, *supra* note 383, at 136-37. For example, password protection can refer to merely an application-layer barrier that a forensic analyst would not encounter, or could refer to an encryption scheme that requires the passphrase to convert ciphertext to plaintext.

481. As one writer explains:

> Because Congress does not have to rely on potentially inconsistent analogies to make law, but instead can undertake exhaustive investigations and studies by experts and gather constituent viewpoints, Congress is in the best position . . . to do just what the Court said was necessary in *Katz*: protect those expectations of privacy "that *society* is prepared to recognize as reasonable.'

Rich Haglund, Note, *Applying Pen Register and Trap and Trace Devices to Internet Communications: As Technology Changes, Is Congress or the Supreme Court Best-Suited to Protect Fourth Amendment Expectations of Privacy?*, 5 VAND. J. ENT. L. & PRAC. 137, 146 (2003) (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

proposed rules in response to concerns of the public, media coverage, or any experts the legislature wishes to consult.[482] Given this environment, the legislative process tends to generate more informed rules governing developing technologies than is likely to result from the closed environment of the judicial process.

F. *The Uniqueness of Criminal Procedure: A Response to Professors Lessig and Sherry, and the Public Choice Theorists*

Up to now, I have focused on the institutional advantages of legislatures over courts. I now turn to the institutional advantages courts may offer over legislatures. Commentators have pointed out two primary advantages of judicial rulemaking in new technologies. The first advantage is that courts can regulate interstitially, making cautious judgments on a case-by-case basis.[483] The second advantage derives from public choice theory; it posits that we cannot trust legislative rules to serve the public interest because legislatures can be captured by special interest groups that engage in rent-seeking.[484] These arguments are persuasive in the context of civil law, but for reasons that follow are much less convincing in the specific context of criminal procedure.

Consider the argument that the interstitial, case-by-case nature of judicial rulemaking is well-suited to regulate new technologies.[485] Much of the scholarship in this area focuses on applying law to the Internet. Professor Lessig suggested in an early article that "the meandering development of the common law"[486] will lead to the best rules for Internet law, especially in the area of First Amendment law. Professor Suzanna Sherry has reached similar conclusions in the context of trademark law and personal jurisdiction.[487] According to Professor Sherry, "the common law method offers the luxury of time

---

482. *See* Kerr, *Internet Surveillance Law After the USA Patriot Act*, *supra* note 323, at 640 (discussing how input from civil libertarian experts changed provisions in the privacy legislation that became the USA PATRIOT Act).

483. *See infra* notes 485 to 490, The classic statement belongs to Holmes: "I recognize without hesitation that judges do and must legislate, but they can do so only interstitially; they are confined from molar to molecular motions." S. Pac. R.R. Co. v. Jensen, 244 U.S. 205, 221 (1917) (Holmes, J., dissenting).

484. *See infra* notes 497 to 498. For a general introduction to public choice theory and the problem of rent-seeking, see DANIEL A. FARBER & PHILIP P. FRICKEY, LAW AND PUBLIC CHOICE: A CRITICAL INTRODUCTION 13-17 (1991); DENNIS C. MUELLER, PUBLIC CHOICE II (1989).

485. *See* NEIL K. KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY 53-97, 123-152 (1994).

486. *See* Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1752 (1995).

487. Suzanna Sherry, *Haste Makes Waste: Congress and the Common Law in Cyberspace*, 55 VAND. L. REV. 309, 309-313 (2002).

and successive experience, while still dealing with the concrete problems posed by the new technology."[488] In contrast, legislative solutions will tend to impose a single approach that will often prove a poor fit for the problem.[489]

These critiques have considerable merit in the context of civil law, the primary focus of Professors Lessig and Sherry. Broadly speaking, civil law regulates private parties interacting with other private parties, and seeks to assign default rules that govern the relationships among them.[490] An important task of the rulemaker is to generate the best background rule. When a technology is new, case-by-case decisionmaking generally leads to a period of uncertain or "muddy" rules.[491] Dan Burk has noted that "muddy" rules in areas of law that involve new technologies encourage parties to contract around ineffective default rules.[492] Burk argues this may be the best possible outcome when technology is in flux; muddy rules allow private parties to resolve background rules through informal bargaining, thus arriving at the best legal solution over time.[493] Case-by-case decisions allow courts to reach tentative decisions along the way until the scope of the problem is better understood and background norms better settled.[494] In effect, case-by-case decisions allow the legal system to grapple with the new technology and try out various informal solutions before a broader resolution emerges through the weight of experience.

I find this argument persuasive in a civil law context, but not in the context of criminal procedure. The case-by-case approach necessarily leaves questions open, and therefore leaves the law uncertain. While this may facilitate bargaining in the civil context, there is no analogous benefit for criminal procedure. Police officers and suspects do not normally negotiate over the rules the police will follow. Either the police will take certain investigative steps or they won't; it is their decision to make based on existing law, not the suspect's. As a result, interstitial rulemaking that leaves the rules unclear lessens the clarity

---

488. *Id.* at 317. Specifically, Professor Sherry argues that Congress should have let the courts answer how trademark law applies to cybersquatting rather than pass a statute (the Anticybersquatting Consumer Protection Act) to decide it.

489. *See id.* at 311 ("[I]n the context of new computer technology, allowing time for incremental judicial responses is often superior to instant legislative solutions of a global nature.").

490. *See, e.g.*, R. H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 9-15 (1960). Of course, this is an enormous oversimplification. For my purposes however, it draws out the essential difference between criminal and civil rules.

491. *See* Dan L. Burk, *Muddy Rules for Cyberspace*, 21 CARDOZO L. REV. 121, 121-25 (1999).

492. *See id.* at 163-178 (outlining the benefits of "muddy" rules involving the Internet, especially in the area of intellectual property law).

493. *See id.*

494. *See* Sherry, *supra* note 487, at 376-377.

of the limits on the government's powers to invade privacy, underdeterring police behavior in some contexts and overdeterring it in others. Legal uncertainty may be a benefit in the civil context, but in the criminal context rule-uncertainty is a liability.[495]

The judicial role in criminal procedure cases also undercuts the benefits of case-by-case decisionmaking because fewer and less-representative issues are likely to pass through the courts. In civil law, the Brownian motion of private parties tends to queue up a diverse range of cases for courts to resolve. Although justiciability doctrines such as standing and ripeness narrow the disputes that courts will hear, the primary barrier to an issue reaching the courts is a plaintiff's decision not to raise it. Different decisions may come up in different ways, letting issues percolate and allowing courts to try different answers to different questions. In criminal law, by contrast, the government holds all the cards. Criminal law follows a top-down model: in federal law, for example, policy is set at the Department of Justice in Washington, D.C. The Department retains broad control over the issues, posture and docket of federal criminal cases.[496] As a result, important legal issues can wait years or even decades before a court is required to pass on them. Recall the history of wiretapping law: no federal court adjudicated the legality of wiretapping until the 1920s, about fifty years after the invention of the telephone. While case-by-case decisions in civil law lets the courts slowly work through the implications of a new technology in fact-specific ways, the same approach in criminal procedure leaves the law unknown until the government opts to push an issue to judicial resolution.

The insights of public choice theory also have only limited force in the context of criminal procedure rules. Public choice theorists have noted that legislative decisions are often influenced by rent-seeking, efforts by interest groups to lobby the government to enact rules that benefit the group at the expense of the public.[497] In contrast, judicial decisionmaking is generally more independent, which in theory can lead to better rules.[498] While these insights have considerable merit in many contexts, they have relatively little force in the context of criminal procedure rules. Privacy and security may be considered public goods, shared equally by the public.[499] The law enforcement

---

495. *See* Bradley, *supra* note 351.

496. *See id.* at 35-39.

497. *See, e.g.*, Jonathan R. Macey, *Public Choice: The Theory of the Firm and the Theory of Market Exchange*, 74 CORNELL L. REV. 43 (1988).

498. *See generally* William M. Landes & Richard A. Posner, *The Independent Judiciary in an Interest Group Perspective*, 18 J.L. & ECON. 875 (1975).

499. As one commentator noted:

> For example, streets which are free from criminal activity offer benefits that are nonexcludable and nonrivalrous. Accordingly, interest groups have little incentive to

interests that might seek "rents" from weak privacy legislation generally do not function as market actors. Governments seek reelection from the public, not greater profits: their interest generally lies more in satisfying the public than in fleecing them. As with all generalizations, exceptions exist. Rules governing civil forfeiture show the effects of rent-seeking: because law enforcement agencies profit from the forfeiture, they have incentives to lobby Congress for broader forfeiture laws.[500] In addition, both law enforcement interests and victims of crime may lobby the legislature for greater enforcement of substantive criminal laws, seeking greater funding and priority among competing interests.[501] But enforcement ordinarily does not impact the contours of criminal procedure rules. In most cases, law enforcement does not "profit" more or less based on how restricted its investigative powers may be, and does not have a clear economic incentive to lobby Congress for less privacy-protecting rules.

It is true that law enforcement groups will often lobby for greater powers. It is also true that law enforcement interests often prove highly influential among legislators.[502] But the former generally reflects honest (if sometimes myopic) claims of the public interest in solving crimes, and the latter generally reflects legitimate public preferences. As William Stuntz has noted, legislators pay careful attention to claims of law enforcement needs precisely because the public demands it.[503] Consider Stuntz's assessment of the influence of law enforcement interests in the context of substantive criminal law:

> Here more than most places, politicians . . . deal with voters directly. And crime is one of those matters about which most voters care a great deal. Today it is regularly a major issue in elections at all levels of government,

---

organize on the ground that the benefits of their collective action would be available to the public at large, yet they would have to bear the entire cost of organization.

Lanier Saperstein, Comment, *Copyrights, Criminal Sanctions and Economic Rents: Applying the Rent Seeking Model to the Criminal Law Formulation Process*, 87 J. CRIM. L. & CRIMINOLOGY 1470, 1471 (1987).

500. *See* Nancy J. King, *Portioning Punishment: Constitutional Limits on Successive and Excessive Penalties*, 144 U. PA. L. REV. 101 188-89 (1995) ("[C]ivil forfeiture may have 'more to do with rent-seeking by legislators and law enforcement officials than with the eradication of drug use.' ") (quoting DONALD J. BOUDREAUX & A.C. PRITCHARD, CIVIL FORFEITURE AND THE WAR ON DRUGS: LESSONS FROM ECONOMICS AND HISTORY 45 (1995)).

501. *See* Saperstein, *supra* note 499 (arguing that the criminal copyright laws reflect rent-seeking from copyright owners).

502. *See* Dripps, *supra* note 336.

503. Stuntz writes:

> Legislators presumably want to stay in office, and perhaps to position themselves for higher office. To do those things, legislators must please their constituents. . . . [F]or most of criminal law, the effect of private interest groups is small: the most important interest groups are usually other government actors, chiefly police and prosecutors.

William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 529 (2001).

> and it has been an issue in local elections for more than a century. If there is any sphere in which politicians would have an incentive simply to please the majority of voters, it's criminal law.
>
> . . . .
>
> Voters may know little about criminal law doctrine, but they presumably have some idea of the set of results they would like to see: conviction and punishment of people who commit the kinds of offenses that voters fear. Legislators, one can fairly hypothesize, have an interest in producing those results (or at least taking credit for them), so that voters will continue to support them.[504]

A similar dynamic is found in the context of criminal procedure. In most circumstances, legislators pay careful attention to law enforcement requests for greater investigative powers because they believe greater powers will enable investigators to solve more crimes.

But what if majoritarian preferences are insufficiently protective of privacy? Donald Dripps has argued that courts must intervene in the area of criminal procedure because statutory criminal procedure rules tend to create intolerable results: in Dripps's words, legislatures "don't . . . give a damn about the rights of the accused."[505] Dripps argues that legislatures cannot create privacy-protective criminal procedure rules because most voters identify themselves as the potential victims of crime rather than its perpetrators.[506] While those who tend to be targeted by the police as suspects may want greater restrictions on law enforcement, those groups tend to be relatively politically powerless.[507] Because politically powerful majorities are more concerned with making sure that criminals are caught, politicians have little to no incentive to protect the rights of the accused.[508] In such circumstances, Dripps argues, we must rely on courts rather than legislatures to generate balanced rules.

There are two reasons to approach this argument with caution. First, Dripps offers only sparse evidence in support of his claim.[509]

---

504. *Id.* at 529-30.

505. Dripps, *supra* note 336, at 1079.

506. *See id.* at 1088-90.

507. *See id.*

508. *See id.*

509. Dripps dismisses the many statutory privacy laws primarily by speculating about Congressional motive; he argues that many if not most of the laws were passed for reasons other than to protect privacy. For example, Dripps suggests that the Wiretap Act was passed not to protect privacy, but to pass constitutional muster: he writes that "the legislative concern behind Title III was not to protect the rights of suspects, but to provide a law enforcement tool that would otherwise by disallowed by the courts." *Id.* at 1083. As Part II demonstrated, it is misleading to understand the passage of the Wiretap Act as solely a product of a wish to provide a tool for law enforcement. Similarly, Dripps explains the passage of the Pen Register statute in 1986 by speculating ". . . that the telephone companies resented the expense and inconvenience of installing [pen register] devices at the whim of

Second, the dynamic Dripps observes may be true in some context but not others, and the case of privacy rules involving developing technologies should provide some reason for optimism. New technologies are often used disproportionately by politically powerful groups. Consider the case of the Internet and the "Digital Divide."[510] The Digital Divide exists because use of computers and the Internet is more widespread among affluent white majorities than among minority groups.[511] A corollary to the Digital Divide is that when Congress legislates in the area of Internet privacy, it is disproportionately legislating the privacy rights of those who are affluent and politically powerful. This will not always be the case. For example, police often have used thermal imaging devices to target marijuana growers. Taken as a whole, however, many criminal investigations involving new technologies will tend to target users of new technologies. Such users generally will be able to represent their interests before Congress effectively, resulting in a healthy debate and relatively favorable conditions for balanced legislative rules.[512]

CONCLUSION

Law professors love constitutional law. Constitutional arguments are particularly popular in the field of criminal procedure because memories of the Warren Court's criminal procedure revolution remain fresh. To many scholars, the Warren Court's decisions reflect the best of what criminal procedure should be — rare bright fixtures in an otherwise dark environment. Having found such a bright light in the courts not long ago, many scholars look to the courts for progress. The existing scholarship on privacy and new technologies reflects this bias

---

police officers, and joined the ACLU in urging that some hurdle be set up between the cop-on-the-beat and the telephone company's time and trouble." *Id.* at 1085. While Dripps is right to note that communications network providers can have a strong influence on privacy legislation affecting those networks, he does not explain whether this is a reason to place more or less trust in the legislative process.

510. *See* Lee Price, *Digital Divide, Digital Opportunities: A Statistical Overview*, 24 HASTINGS COMM. & ENT. L.J. 567 (2002) (exploring the gap in computer use among different communities in the United States).

511. *Id.*

512. Polls taken since September 11, 2001, appear to confirm this. Post-9/11 Harris Polls suggest that the public is divided over the scope of the government's high-tech surveillance powers, but that the existing statutory rules are probably slightly more privacy protecting than the majority public preference would wish. *See Homeland Security: American Public Continues to Endorse a Broad Range of Proposals for Stronger Surveillance Powers, but Support Has Declined Somewhat*, THE HARRIS POLL #14, March 10, 2003 (*available at* www.harrisinteractive.com/harris_poll/index.asp?PID=362). The polls suggest that about 60% of the public would favor expanded camera surveillance, about 55% would favor law enforcement monitoring of Internet chat rooms, and about 45% of the public would favor expanded government monitoring of cell phones and e-mail. *Id.* While these numbers are merely one data point in a complex matrix, they seem to suggest that in the area of high-technology privacy, the legislative process is likely operating reasonably effectively.

in favor of constitutional argument. The scholarship focuses on the Fourth Amendment and the judiciary as the primary source of rules to regulate uses of new technology.

This article has argued that the judiciary-focused view overlooks the critical role that statutory privacy protections have played in protecting privacy in developing technologies. It has argued that legislatures often are better situated than courts to protect privacy in new technologies, and that courts should be wary of imposing broad privacy protections against the government's use of new technologies in light of the judiciary's institutional difficulties. Indeed, the courts and Congress may be far ahead of the game already. While scholars have unsuccessfully urged courts to adopt expansive visions of the Fourth Amendment in new technologies, Congress has quietly assumed the leading role in that endeavor. Today the rules governing law enforcement use of new technologies tend to be statutory rules, not constitutional ones. Traditional cases with stable technologies tend to be regulated by the Fourth Amendment, but cases with developing technologies tend to be regulated by statute.

As technology advances and the difficulty courts face regulating privacy in new technologies becomes clearer, this trend toward statutory protections will likely accelerate. In time, we may understand the law of criminal procedure as a bifurcated field, with constitutional rules governing most traditional cases and statutory rules governing most cases involving new technologies. New technologies may reveal the limits of the modern enterprise of constitutional criminal procedure, making the field part constitutional and part statutory. The potential bifurcation of criminal procedure will pose a significant challenge to scholars of criminal procedure. Increasingly, an understanding of criminal procedure may require an understanding of complicated statutory provisions. The criminal procedure curriculum may change as well. The study of statutory privacy laws may work its way into courses currently dedicated to constitutional protections. Alternatively, new classes may appear to cover statutory privacy laws not covered elsewhere. Either way, developing technologies may well push criminal procedure to change from a primarily constitutional field to a more mixed field, and the scholarship will have to change along with it to stay relevant to law enforcement practice and judicial experience.